

POINTED p^3 -DIMENSIONAL HOPF ALGEBRAS IN POSITIVE CHARACTERISTIC

VAN C. NGUYEN AND XINGTING WANG

ABSTRACT. We classify pointed p^3 -dimensional Hopf algebras H over any algebraically closed field \mathbf{k} of prime characteristic $p > 0$. In particular, we focus on the cases when the group $G(H)$ of group-like elements is of order p or p^2 , that is, when H is pointed but is not connected nor a group algebra. This work provides many new examples of (parametrized) non-commutative and non-cocommutative finite-dimensional Hopf algebras in positive characteristic.

INTRODUCTION

The classification of pointed p^3 -dimensional Hopf algebras H in characteristic zero (e.g. in \mathbb{C}) was independently presented by Andruskiewitsch and Schneider [2, 3, 4], by Caenepeel and Dăscălescu [8], and by Stefan and van Oystaeyen [22] using different methods. In this paper, we provide the classification in characteristic $p > 0$. This work, together with the classification of connected p^3 -dimensional Hopf algebras [15, 16] and that of groups of order p^3 , provides isomorphism classes of pointed Hopf algebras of dimension p^3 over an algebraically closed field of characteristic p .

Moreover, we remark that the classification of p^n -dimensional pointed Hopf algebras over an algebraically closed field of prime characteristic $q > 0$, where p and q are coprime, yields similar isomorphism classes as in the case of characteristic zero; since the same technique should work in both cases. Hence, our work in this paper in characteristic $p > 0$, combined with previous classification results by other authors, will complete the classification picture for pointed Hopf algebras of dimensions p, p^2 , and p^3 over any algebraically closed field of *arbitrary* characteristic.

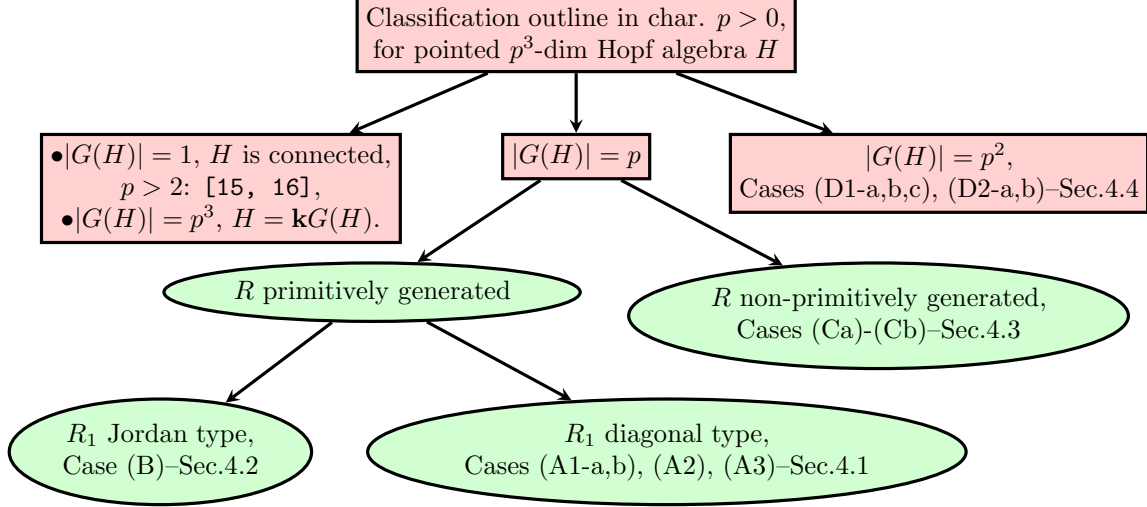
We present the following diagram outlining our classifying idea in this paper. We first break down to smaller cases by the order of the group $G(H)$ of grouplike elements. We observe that in the case when $|G(H)| = p$, it occurs that the braided Hopf algebra R in the associated graded Hopf algebra $\text{gr } H \cong R \# \mathbf{k}G(H)$ of H , cf. Section 1, may not be primitively generated, and we could have Yetter-Drinfeld modules in ${}^G\mathcal{YD}$ of either diagonal type or Joran type; hence, further cases occur where the structures arise. Interested readers may refer to corresponding section(s) for detailed classification results.

At last, we emphasize that the principle proposed by Andruskiewitsch and Schneider in [2] to study pointed Hopf algebras in characteristic zero is generally applicable

2010 *Mathematics Subject Classification.* 16T05, 17B60.

Key words and phrases. braided Hopf algebras, Yetter-Drinfeld modules, positive characteristic, pointed Hopf algebras, Nichols algebras.

in positive characteristic. But the difficulty arises when the characteristic of the base field \mathbf{k} divides the dimension of the pointed Hopf algebra H , because in this situation: (1) the braided Hopf algebras R are in general not primitively generated (that is, they are not Nichols algebras) even when $G(H)$ is abelian, and (2) the liftings from $\text{gr } H$ to H are computationally challenging in characteristic p .



We obtain the following classes of pointed p^3 -dimensional Hopf algebras in characteristic $p > 0$:

Case A1. Liftings from $\text{gr } H = \mathbf{k}\langle a, b, g \rangle / (g^p = 1, a^p = b^p = 0, ab = ba, ga = ag, gb = bg)$, with $\Delta(g) = g \otimes g$, $\Delta(a) = a \otimes 1 + g \otimes a$, $\Delta(b) = b \otimes 1 + g^u \otimes b$, $\varepsilon(g) = 1$, $\varepsilon(a) = \varepsilon(b) = 0$, $S(g) = g^{-1}$, $S(a) = -ag^{-1}$, $S(b) = -bg^{-u}$, for $0 \leq u \leq p-1$.

When $u = 0$, there are 1 infinite parametric family and 10 finite classes of H having structured lifted from case (A1). When $u \neq 0$, there are $2(p-1)$ infinite parametric families and $6(p-1)$ finite classes of H .

Case A2. Liftings from $\text{gr } H = \mathbf{k}\langle a, b, g \rangle / (g^p = 1, a^p = b^p = 0, ab = ba, ga = ag, gb = bg)$, with $\Delta(g) = g \otimes g$, $\Delta(a) = a \otimes 1 + 1 \otimes a$, $\Delta(b) = b \otimes 1 + 1 \otimes b$, $\varepsilon(g) = 1$, $\varepsilon(a) = \varepsilon(b) = 0$, $S(g) = g^{-1}$, $S(a) = -a$, $S(b) = -b$.

There are 5 finite classes of H having structured lifted from case (A2).

Case A3. ($p = 2$) Liftings from $\text{gr } H = \mathbf{k}\langle a, b, g \rangle / (g^p = 1, a^p = b^p = 0, ab = ba, ga = bg, gb = ag)$, with $\Delta(g) = g \otimes g$, $\Delta(a) = a \otimes 1 + 1 \otimes a$, $\Delta(b) = b \otimes 1 + 1 \otimes b$, $\varepsilon(g) = 1$, $\varepsilon(a) = \varepsilon(b) = 0$, $S(g) = g^{-1}$, $S(a) = -a$, $S(b) = -b$.

There are 5 finite classes of H having structured lifted from case (A3).

Case B. ($p > 2$) Liftings from $\text{gr } H = \mathbf{k}\langle a, b, g \rangle / (g^p = 1, a^p = b^p = 0, ab - ba = \frac{1}{2}a^2, ga = ag, gb = (a + b)g)$, with $\Delta(g) = g \otimes g, \Delta(a) = a \otimes 1 + g \otimes a, \Delta(b) = b \otimes 1 + g \otimes b, \varepsilon(g) = 1, \varepsilon(a) = \varepsilon(b) = 0, S(g) = g^{-1}, S(a) = -ag^{-1}, S(b) = (a - b)g^{-1}$.

Due to complicated computations in characteristic p , the lifting in case (B) is not clear in general; however, we show in Section 4.2 the case when $p = 3$ for illustration and make a conjecture for the lifting for $p > 3$.

Case C. Liftings from $\text{gr } H = \mathbf{k}\langle a, b, g \rangle / (g^p = 1, a^p = b^p = 0, ab = ba, ga = ag, gb = bg)$, with $\Delta(g) = g \otimes g, \Delta(a) = a \otimes 1 + g^\epsilon \otimes a, \Delta(b) = b \otimes 1 + 1 \otimes b + \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} (a^i g^{\epsilon(p-i)} \otimes a^{p-i}), \varepsilon(g) = 1, \varepsilon(a) = \varepsilon(b) = 0, S(g) = g^{-1}, S(a) = -ag^{-\epsilon}, S(b) = -b$, for $\epsilon \in \{0, 1\}$.

When $\epsilon = 0$, we get 1 infinite parametric family and 2 finite classes of H . When $\epsilon = 1$, due to complicated computations in characteristic p , the lifting in this case (Cb) is not clear in general. We show in Section 4.3 the cases (C) when $p = 2$, and when $p > 2$ with additional assumption $gx = xg$, where x is the lifting of a from $\text{gr } H$ to H .

Case D1. Liftings from $\text{gr } H = \mathbf{k}\langle a, g \rangle / (g^{p^2} = 1, a^p = 0, ga = ag)$, with $\Delta(g) = g \otimes g, \Delta(a) = a \otimes 1 + g^\epsilon \otimes a, \varepsilon(g) = 1, \varepsilon(a) = 0, S(g) = g^{-1}, S(a) = -ag^{-\epsilon}$, for $\epsilon \in \{0, 1, p\}$.

When $\epsilon = 0$, we get 2 finite classes of H . When $\epsilon = 1$, there are 1 infinite parametric family and 2 finite classes of H . When $\epsilon = p$, there are 2 finite classes of H .

Case D2. Liftings from $\text{gr } H = \mathbf{k}\langle a, g_1, g_2 \rangle / (g_1^p = g_2^p = 1, a^p = 0, g_i a = a g_i)$, with $\Delta(g_i) = g_i \otimes g_i, \Delta(a) = a \otimes 1 + g_1^\epsilon \otimes a, \varepsilon(g_i) = 1, \varepsilon(a) = 0, S(g_i) = g_i^{-1}, S(a) = -ag_1^{-\epsilon}$, for $\epsilon \in \{0, 1\}$.

When $\epsilon = 0$, we have 2 finite classes of H . When $\epsilon = 1$, there are 1 infinite parametric family and 2 finite classes of H .

The paper is organized as follows. In Section 1, we recall some basic notations and properties of pointed Hopf algebras, Yetter-Drinfeld modules and Nichols algebras. In Section 2, we study rank two Nichols algebras over $\mathbf{k}G$ where \mathbf{k} is of arbitrary characteristic and G is a finite group. In Section 3, we study the bosonizations of these braided Hopf algebras under the assumption that \mathbf{k} is of characteristic p and G is a p -group of order $\leq p^2$. In Section 4, we apply the Lifting Method to these bosonizations to obtain our classification results. Finally, we point out that rank two Nichols algebras of diagonal type over fields of positive characteristic were studied in [11]; and the Nichols algebras in Case (B) were first discussed in [9] as examples of Nichols algebras in positive characteristic.

1. PRELIMINARY

We first recall some general results over a base field \mathbf{k} of arbitrary characteristic. The unadorned tensor \otimes means $\otimes_{\mathbf{k}}$ unless specified otherwise. Let $H := H(m, u, \Delta, \varepsilon, S)$ be any finite-dimensional pointed Hopf algebra with its *coradical* H_0 (the sum of all simple subcoalgebras of H) a group algebra $H_0 = \mathbf{k}G$; that is, H_0 is a Hopf subalgebra of H generated by the grouplike elements $G := G(H) = \{g \in H \mid \Delta(g) = g \otimes g\}$. Note that the dimension of H_0 (and hence the order of group G) must divide the dimension of H by Nichols-Zoeller's freeness theorem [17].

Let

$$H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H$$

be the *coradical filtration* of H , where $H_n = \Delta^{-1}(H \otimes H_{n-1} + H_0 \otimes H)$ inductively, see [14, Chapter 5]. For pointed Hopf algebras H , this is indeed a Hopf algebra filtration since the coradical $H_0 = \mathbf{k}G$ is a Hopf subalgebra of H [14, Lemma 5.2.8]. Hence, we can consider the associated graded Hopf algebra $\text{gr } H = \bigoplus_{n \geq 0} H_n / H_{n-1}$, with convention $H_{-1} = 0$. Note that the zero term of $\text{gr } H$ equals its coradical, i.e. $(\text{gr } H)_0 = H_0$. There is a projection $\pi : \text{gr } H \rightarrow H_0$ and an inclusion $\iota : H_0 \rightarrow \text{gr } H$ such that $\pi\iota = \text{id}_{H_0}$. Let R be the algebra of coinvariants of π :

$$R := (\text{gr } H)^{\text{co}\pi} = \{h \in \text{gr } H : (\text{id} \otimes \pi)\Delta(h) = h \otimes 1\}.$$

By a result of Radford [18] and Majid [13], R is a graded braided Hopf algebra, that is, it is a Hopf algebra in the braided category ${}^G\mathcal{YD}$ of left Yetter-Drinfeld modules over $H_0 = \mathbf{k}G$. Moreover, $\text{gr } H$ is the *bosonization* (or *Radford biproduct*) of R and H_0 such that $\text{gr } H \cong R \# H_0$ with the following Hopf structure [14, Theorem 10.6.5]:

- underlying vector space is the tensor product $R \otimes H_0$,
- multiplication $(r \# g)(r' \# g') = r(g \cdot r') \# (gg')$,
- comultiplication $\Delta(r \# g) = \sum r^{(1)} \# (r^{(2)})_{(-1)} g \otimes (r^{(2)})_{(0)} \# g$,
- counit $\varepsilon(r \# g) = \varepsilon_R(r) \varepsilon_G(g) = \varepsilon_R(r)$,
- antipode $S(r \# g) = \sum (1 \# S_G(r_{(-1)} g)) (S_R(r_{(0)}) \# 1)$,

for all $r, r' \in R$ and $g, g' \in G$. Here, we use the Sweedler notation $\Delta_R(r) = \sum r^{(1)} \otimes r^{(2)}$ for the comultiplication of R ; and the H_0 -coaction on R , $\rho_R : R \rightarrow H_0 \otimes R$, is given by $\rho_R(r) = \sum r_{(-1)} \otimes r_{(0)}$. In this case, the Hopf algebra projection $\pi : R \# H_0 \rightarrow H_0$ and inclusion $\iota : H_0 \rightarrow R \# H_0$ are given by $\pi(r \# g) = \varepsilon(r)g$ and $\iota(g) = 1 \# g$, respectively.

Our strategy, following the principle proposed in [2], is as follows: to study H , given $H_0 = \mathbf{k}G$, we will first study R as a Hopf algebra in ${}^G\mathcal{YD}$, then transfer its structures to $\text{gr } H$ via the bosonization $R \# H_0$, and finally we lift $\text{gr } H$ structures to H via the filtration. We present the classification of pointed p^3 -dimensional Hopf algebras H in characteristic $p > 0$ in Sections 3 and 4 of this paper.

1.1. Yetter-Drinfeld modules. We say that a vector space V is a left Yetter-Drinfeld module over $\mathbf{k}G$ if V is both a $\mathbf{k}G$ -module and $\mathbf{k}G$ -comodule satisfying

$$\rho_V(g \cdot v) = \sum g v_{(-1)} g^{-1} \otimes g \cdot v_{(0)},$$

for all $v \in V$ and $g \in G$. We denote by $\rho_V : V \rightarrow \mathbf{k}G \otimes V$ the G -coaction on V such that $\rho_V(v) = \sum v_{(-1)} \otimes v_{(0)}$, for any $v \in V$. Since V is a $\mathbf{k}G$ -comodule, $V = \bigoplus_{g \in G} V_g$ such that for any homogenous element $v \in V_g$ we have $\rho_V(v) = g \otimes v$, for $g \in G$. We call g the G -grading of $v \in V_g$. In particular, for an abelian group G , any Yetter-Drinfeld module $V \in {}^G_G\mathcal{YD}$ is a G -graded $\mathbf{k}G$ -module, i.e. $V = \bigoplus_{g \in G} V_g$ such that each V_g is a $\mathbf{k}G$ -submodule of V .

We denote by ${}^G_G\mathcal{YD}$ the category of all left Yetter-Drinfeld modules over $\mathbf{k}G$, where the morphisms are both G -linear and G -colinear maps. In general, the category ${}^G_G\mathcal{YD}$ is a braided monoidal (tensor) category. That is, for any $V, W \in {}^G_G\mathcal{YD}$, $V \otimes W$ is again an object of ${}^G_G\mathcal{YD}$ via action $g \cdot (v \otimes w) = \Delta(g)(v \otimes w) = (g \cdot v) \otimes (g \cdot w)$, for all $g \in G, v \in V$, and $w \in W$. The braiding structure is given by twisting maps $c_{V,W} : V \otimes W \rightarrow W \otimes V$, which is an isomorphism in the category ${}^G_G\mathcal{YD}$:

$$c_{V,W}(v \otimes w) = \sum v_{(-1)} \cdot w \otimes v_{(0)}$$

with inverse

$$c_{V,W}^{-1}(w \otimes v) = \sum v_{(0)} \otimes S^{-1}(v_{(-1)}) \cdot w,$$

for all $v \in V$ and $w \in W$.

Let A, B be two \mathbf{k} -algebras in the category ${}^G_G\mathcal{YD}$, the tensor product $A \otimes B$ is again a \mathbf{k} -algebra in ${}^G_G\mathcal{YD}$ with multiplication given by $m_{A \otimes B} = (m_A \otimes m_B)(\text{id}_A \otimes c_{B,A} \otimes \text{id}_B)$ satisfying:

$$1_{A \otimes B} = 1_A \otimes 1_B \quad \text{and} \quad (a \otimes b)(a' \otimes b') = a(b_{(-1)} \cdot a') \otimes b_{(0)}b'$$

for all $a, a' \in A$ and $b, b' \in B$.

1.2. Braided Hopf algebra R . Following the above notations, we say that R is a braided Hopf algebra in the category ${}^G_G\mathcal{YD}$ of Yetter-Drinfeld modules over group algebra $H_0 = \mathbf{k}G$, with the following structures (c.f. [3, §1]):

- The action of H_0 on R is given by the adjoint action composed with the inclusion $\iota : H_0 \rightarrow \text{gr } H$. The coaction of H_0 on R is given by $\rho_R = (\pi \otimes \text{id})\Delta : R \rightarrow H_0 \otimes R$.
- R is a Hopf algebra in ${}^G_G\mathcal{YD}$: it is a subalgebra of $\text{gr } H$ and a coalgebra with comultiplication $\Delta_R(r) = r_{(1)}\iota\pi S(r_{(2)}) \otimes r_{(3)}$ and antipode $S_R(r) = \iota\pi(r_{(1)})S(r_{(2)})$, for all $r \in R$.

Observe that R inherits the usual \mathbb{N} -grading from $\text{gr } H$, so $R = \bigoplus_{n \geq 0} R_n$ is a graded braided Hopf algebra, where each $R_n := R \cap (\text{gr } H)_n$ is a Yetter-Drinfeld submodule of R over $H_0 = \mathbf{k}G$. Let $V = \{r \in R \mid \Delta_R(r) = r \otimes 1 + 1 \otimes r\}$ be the space of primitive elements of R . By the discussion in [2, §2], we have $\text{gr } H$ is coradically graded, and it follows that $V = R_1$, that is, all primitive elements of R has degree 1 in R [2, Lemma 2.4]. Moreover, V is a Yetter-Drinfeld submodule of R and its braiding $c := c_{V,V} : V \otimes V \rightarrow V \otimes V$ is called the *infinitesimal braiding* of H . The dimension of V is called the *rank* of H . The subalgebra $\mathcal{B}(V)$ of R generated over \mathbf{k} by V is a braided Hopf subalgebra whose structure only depends on the infinitesimal braiding of V , called the *Nichols algebra* of V , c.f. [3, §2].

We remark here that the structure of R in characteristic $p > 0$ is different than that in characteristic zero: There is a long-standing conjecture by Andruskiewitsch and Schneider, e.g. [3, Conjecture 2.7], that in characteristic zero, if H_0 is an abelian group algebra then R is always primitively generated, $R = \langle R_0 \oplus R_1 \rangle$. This is proved by Angiono and Iglesias in [5, Theorem 2.6] for the case in which the infinitesimal braiding is of standard type. Thus, in such case, $R = \mathcal{B}(V)$, the Nichols algebra of the Yetter-Drinfeld submodule $V = R_1$. However, in characteristic $p > 0$, R may not be primitively generated in general and there may exist non-primitive generator(s) in R , e.g. [3, Example 2.5]. We will consider an example of this case later in Section 3.2.

1.3. Simple and indecomposable ${}_{\mathcal{C}}\mathcal{YD}$ -modules. Let \mathbf{k} be a base field of arbitrary characteristic and G be any finite group. We look at the simple and indecomposable Yetter-Drinfeld modules over $\mathbf{k}G$. This work has been previously discussed by other authors such as [1, Proposition 3.1.2] and [12, Corollary 3.2]. We present here a ring-theoretical approach, independent of the characteristic of the field \mathbf{k} .

Recall that the *Drinfeld (quantum) double* $D(H)$ of any finite-dimensional Hopf algebra H over \mathbf{k} is again a Hopf algebra and is defined as follows. As a coalgebra, $D(H) = H^{*cop} \otimes H$, where $H^* = \text{Hom}_{\mathbf{k}}(H, \mathbf{k})$ is the vector space dual of H which is again a Hopf algebra, and the comultiplication of H^{*cop} is opposite to that of H^* . Denote $f \otimes x$ by $f \bowtie x \in D(H)$, for any $f \in H^{*cop} = H^*$ and $x \in H$, then the multiplication in $D(H)$ is given by

$$(f \bowtie x)(g \bowtie y) = \sum f(x_{(1)} \rightharpoonup g \leftharpoonup S^{-1}(x_{(3)})) \bowtie (x_{(2)}y),$$

for any $f, g \in H^{*cop} = H^*$ and $x, y \in H$, where $x \rightharpoonup g$ and $g \leftharpoonup x \in H^{*cop} = H^*$ are defined as:

$$\langle x \rightharpoonup g, y \rangle = \langle g, yx \rangle, \quad \langle g \leftharpoonup x, y \rangle = \langle g, xy \rangle.$$

For any finite group G , we have $D(G) := D(\mathbf{k}G) = \mathbf{k}^G \# \mathbf{k}G$, where $\mathbf{k}^G := (\mathbf{k}G)^* = \text{Span}\{\delta_g \mid g \in G\}$, with action of $\mathbf{k}G$ on \mathbf{k}^G via $g \cdot \delta_h = \delta_{ghg^{-1}}$, for any $g \in G$ and $\delta_h \in \mathbf{k}^G$. In particular, $D(G)$ is generated by all choices of $g = (\varepsilon \bowtie g)$ and $\delta_h = (\delta_h \bowtie 1_G)$, for $g, h \in G$, satisfying $g\delta_h = (\varepsilon \bowtie g)(\delta_h \bowtie 1_G) = \delta_{ghg^{-1}} \bowtie g$.

Let $G = \sqcup_{i=1}^n \mathcal{O}_i$ be the conjugacy class decomposition of G . We see that $\mathbf{k}^{\mathcal{O}_i} = \text{Span}\{\delta_h \mid h \in \mathcal{O}_i\}$ is a subring of \mathbf{k}^G . Clearly from the definition, we have

Lemma 1.3.1. $D(G) \cong \bigoplus_{i=1}^n (\mathbf{k}^{\mathcal{O}_i} \# \mathbf{k}G)$ as finite-dimensional algebras.

Let R be any ring and $e \in R$ be an idempotent of R such that $ReR = R$.

Lemma 1.3.2. *The two categories $R\text{-Mod}$ and $eRe\text{-Mod}$ are Morita equivalent.*

Proof. Consider the Schur functor $F : R\text{-Mod} \rightarrow eRe\text{-Mod}$ and its natural inverse $G : eRe\text{-Mod} \rightarrow R\text{-Mod}$, defined via $F : M \mapsto eR \otimes_R M$ and $G : N \mapsto Re \otimes_{eRe} N$. It is easy to check from the construction that $GF = \text{id}_{R\text{-Mod}}$ and $FG = \text{id}_{eRe\text{-Mod}}$. \square

Lemma 1.3.3. *In each finite-dimensional algebra $R = \mathbf{k}^{\mathcal{O}_i} \# \mathbf{k}G$, we denote idempotent $e = (\delta_g \# 1_G)$, for any choice of $g \in \mathcal{O}_i$. Then:*

- (a) $1_R = (\sum_{h \in \mathcal{O}_i} \delta_h) \# 1_G$.
- (b) $ReR = R$.

(c) $eRe \cong \mathbf{k}C(g)$, where $C(g)$ is the centralizer of g in G .

Proof. Fix any choice of $g \in \mathcal{O}_i$, it is clear that $e = (\delta_g \# 1_G) = (\delta_g \# 1_G)(\delta_g \# 1_G) = e^2$ is an idempotent.

(a) Write $\text{id} = \sum_{h \in \mathcal{O}_i} \delta_h$. It is clear that $\text{id}\delta_h = \delta_h\text{id} = \delta_h$ for any $h \in \mathcal{O}_i$. Thus $\text{id} \# 1_G$ is the identity.

(b) Observe that for any $h, h' \in G$, $(\text{id} \# h)(\delta_g \# 1_G)(\text{id} \# h') = (\delta_{hgh^{-1}} \# hh')$. By varying all choices of $h, h' \in G$, this identity will give us all of $(\mathbf{k}^{\mathcal{O}_i} \# \mathbf{k}G)$.

(c) For any $\delta_h \in \mathbf{k}^{\mathcal{O}_i}$ and $h' \in G$,

$$\begin{aligned} (\delta_g \# 1_G)(\delta_h \# h')(\delta_g \# 1_G) &= \delta_g \delta_h \delta_{h'g(h')^{-1}} \# h' \\ &= \begin{cases} 0, & h \neq g \text{ or } h'g(h')^{-1} \neq g, \\ \delta_g \# h', & h = g \text{ and } h' \in C(g). \end{cases} \end{aligned}$$

Since g is fixed, by identifying $\delta_g \# h' \leftrightarrow h'$, we obtain the statement as claimed. \square

The following results follow from Lemmas 1.3.1 and 1.3.2:

Corollary 1.3.4. (a) *The two categories $(\mathbf{k}^{\mathcal{O}_i} \# \mathbf{k}G)\text{-Mod}$ and $\mathbf{k}C(g)\text{-Mod}$ are Morita equivalent, for any $g \in \mathcal{O}_i$.*

(b) *$D(G)\text{-Mod}$ is Morita equivalent to $(\bigoplus_{i=1}^n \mathbf{k}C(g_i))\text{-Mod}$, for any choice of $g_i \in \mathcal{O}_i$. As a consequence, there are bijections between*

$$\{\text{simple } D(G)\text{-modules}\} \longleftrightarrow \sqcup_{1 \leq i \leq n} \{\text{simple } \mathbf{k}C(g_i)\text{-modules}\},$$

and

$$\{\text{indecomposable } D(G)\text{-modules}\} \longleftrightarrow \sqcup_{1 \leq i \leq n} \{\text{indecomposable } \mathbf{k}C(g_i)\text{-modules}\}.$$

It is well-known that the category of Yetter-Drinfeld modules ${}^G\mathcal{YD}$ is equivalent to the category of left $D(G)$ -modules for any finite group G . The above bijections can then be written in details so that every simple (resp. indecomposable) ${}^G\mathcal{YD}$ -module is given in the form of $\mathbf{k}G \otimes_{C(g_i)} M$, for some $g_i \in \mathcal{O}_i$ and some simple (resp. indecomposable) module M over $C(g_i)$. Moreover, the $\mathbf{k}G$ -module structure is given as the induced module $(\mathbf{k}G \otimes_{C(g_i)} -)$ and the $\mathbf{k}G$ -comodule structure is given by $\rho(x \otimes m) = xg_ix^{-1} \otimes (x \otimes m)$, for any $(x \otimes m) \in \mathbf{k}G \otimes_{C(g_i)} M$.

Remark 1.3.5. Let G be a finite p -group, and $\text{char. } \mathbf{k} = p > 0$. Then every simple module in ${}^G\mathcal{YD}$ is of the form $\mathbf{k}G \otimes_{C(g_i)} \mathbf{k}$, where \mathbf{k} is the trivial module over $C(g_i)$, for some choice $g_i \in \mathcal{O}_i$ and $\rho(x \otimes 1) = xg_ix^{-1} \otimes (x \otimes 1)$, for any $x \in G$. In particular, if $G = C_p$ is a cyclic group of prime order p and $\text{char. } \mathbf{k} = p$, then every simple ${}^G\mathcal{YD}$ -module is one-dimensional with trivial G -action and some G -grading.

1.4. Braiding types of ${}^G\mathcal{YD}$ -modules and Nichols algebras. A full description of Nichols algebras is given in e.g. [3, §2 and §3]. Here, we only focus on the case with $H_0 = \mathbf{k}G$ and G is a finite group. Let V be a Yetter-Drinfeld module in ${}^G\mathcal{YD}$ of finite dimension d with fixed basis $\{x_1, x_2, \dots, x_d\}$. Let $\chi : G \rightarrow \mathbf{k}$ be any character on G . We denote

$$V_g := \{x \in V \mid \rho(x) = g \otimes x\}, \quad V^\chi := \{x \in V \mid g \cdot x = \chi(g)x, g \in G\}.$$

The support of V is defined to be

$$\text{supp}(V) := \{g \in G \mid V_g \neq 0\}$$

and we denote by G_V the subgroup of G generated by $\text{supp}(V)$. Note that we can consider V as a Yetter-Drinfeld module over G_V by natural restriction.

There are two types of braiding $c : V \otimes V \rightarrow V \otimes V$ in which we are interested in this paper:

- $V = \mathcal{D}(d)$ is of *diagonal type*:

$$c(x_i \otimes x_j) = q_{ij} x_j \otimes x_i,$$

for all $1 \leq i, j \leq d$, where $q_{ij} \in \mathbf{k}^\times$. We call $\mathbf{q} = (q_{ij})_{1 \leq i, j \leq d}$ the braiding matrix. Moreover, we say that a braided vector space (V, c) of diagonal type is *realizable* as some Yetter-Drinfeld module in ${}^G\mathcal{YD}$ if V admits a *principal \mathcal{YD} -realization*, that is, if we can find a family $(g_i, \chi_i)_{1 \leq i \leq d}$ of elements $g_i \in Z(G)$ and characters $\chi_i \in \widehat{G}$ such that $\chi_j(g_i) = q_{ij} \in \mathbf{k}^\times$, for all $1 \leq i, j \leq d$. In this case, we can consider V as a Yetter-Drinfeld module in ${}^G\mathcal{YD}$ by defining $x_i \in V_{g_i}^{\chi_i} = V_{g_i} \cap V^{\chi_i}$, for all $1 \leq i \leq d$, [6, §2].

- One important example of the non-diagonal types is the Jordan type. We say $V = \mathcal{J}(t, d)$ is of *Jordan type*, which only happens when $d \geq 2$:

$$c(x_i \otimes x_1) = tx_1 \otimes x_i \quad \text{and} \quad c(x_i \otimes x_j) = (tx_j + x_{j-1}) \otimes x_i,$$

for all $1 \leq i \leq d, 2 \leq j \leq d$, and some $t \in \mathbf{k}^\times$. The braiding matrix is of the form:

$$\begin{pmatrix} t & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & t & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & t & \cdots & 0 & 0 & 0 \\ \vdots & & & \ddots & & & \vdots \\ 0 & 0 & 0 & \cdots & t & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & t & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & t \end{pmatrix}_{d \times d}$$

We say that the braided vector space (V, c) of Jordan type is *realizable* as some Yetter-Drinfeld module in ${}^G\mathcal{YD}$ if V admits a *non-principal \mathcal{YD} -realization*, that is, if we can find a pair $(\varphi, g) \in \text{rep}_d(G) \times Z(G)$ such that each basis x_i has the same G -grading via coaction $\rho(x_i) = g \otimes x_i$, and $\varphi : G \rightarrow \text{GL}(V)$ is a representation of G on V satisfying $\varphi(g) \cdot x_1 = tx_1$ and $\varphi(g) \cdot x_i = tx_i + x_{i-1}$ for all $2 \leq i \leq d$.

Note that the Nichols algebra $\mathcal{B}(V)$ is uniquely determined by the braiding c , so $\mathcal{B}(V)$ only depends on the (co)actions of G on V as described in above cases.

Proposition 1.4.1. *Let G be a finite group, and (V, c) be a Yetter-Drinfeld module over G of dimension $d < \infty$. Then*

- (1) *(V, c) is of diagonal type if V is a direct sum of one-dimensional Yetter-Drinfeld modules over G_V . Moreover, V has a principal \mathcal{YD} -realization if*

and only if V is a direct sum of one-dimensional Yetter-Drinfeld modules over G .

- (2) (V, c) is of Jordan type if there is some central group element $g \in G$ and $t \in \mathbf{k}^\times$ such that all elements in V have the same G -grading given by g and the minimal polynomial for the g -action on V is $(g - t)^d$, with $d = \dim V \geq 2$.

Proof. (1) View V as a Yetter-Drinfeld module over G_V . Suppose $V = \bigoplus_{1 \leq i \leq d} V_i$ is a direct sum of one-dimensional Yetter-Drinfeld modules over G_V . Let x_j be a basis for V_j , for all $1 \leq j \leq d$. Then one sees that, for any V_j , the G_V -action is given by some character $\chi_j : G_V \rightarrow \mathbf{k}$ such that $h \cdot x_j = \chi_j(h)x_j$, for any $h \in G_V$; and the G_V -coaction is given by some central element $g_j \in G_V$ such that $\rho(x_j) = g_j \otimes x_j$. As a consequence, V is of diagonal type with braiding matrix given by $\mathbf{q} = (q_{ij})_{1 \leq i, j \leq d}$ with $q_{ij} = \chi_j(g_i)$. The argument for principal \mathcal{YD} -realization is similar.

(2) Suppose there are $g \in Z(G)$ and $t \in \mathbf{k}^\times$ such that all elements in V are of the same G -grading g and the minimal polynomial for the g -action on V is $(g - t)^d$ with $d = \dim V \geq 2$. It follows from the Jordan block decomposition that there exists a basis x_1, \dots, x_d such that $g \cdot x_1 = tx_1$ and $g \cdot x_j = tx_j + x_{j-1}$, for all $2 \leq j \leq d$. Then it is clear that the braiding of V associated to this basis is of Jordan type. \square

1.5. Hochschild cohomology of Nichols algebras. Let G be a finite group, and V be a Yetter-Drinfeld module over G . Denote by $\mathcal{B}(V)$ the Nichols algebra of V , which is a connected graded braided Hopf algebra in ${}^G\mathcal{YD}$. We will use the cobar construction on $\mathcal{B}(V)$ (cf. [23]), denoted by $\Omega\mathcal{B}(V)$, to compute its Hochschild cohomology.

- As graded algebras, $\Omega\mathcal{B}(V) = T(\mathcal{B}(V)^+)$ is the tensor algebra of $\mathcal{B}(V)^+ := \{\text{all grading } \geq 1 \text{ parts of } \mathcal{B}(V)\}$.
- The differentials $\partial^n : (\mathcal{B}(V)^+)^{\otimes n} \rightarrow (\mathcal{B}(V)^+)^{\otimes(n+1)}$ are given by

$$\partial^n = \sum_{i=0}^{n-1} (-1)^{i+1} 1^{\otimes i} \otimes \overline{\Delta} \otimes 1^{\otimes(n-i-1)},$$

where $\overline{\Delta}(r) = \Delta(r) - r \otimes 1 - 1 \otimes r$, for any $r \in \mathcal{B}(V)^+$.

The differentials in low degrees are explicitly given as follows:

$$\partial^1(x) = \Delta(x) - x \otimes 1 - 1 \otimes x,$$

$$\partial^2(x \otimes y) = 1 \otimes x \otimes y - \Delta(x) \otimes y + x \otimes \Delta(y) - x \otimes y \otimes 1$$

for $x, y \in \mathcal{B}(V)^+$. The i -th Hochschild cohomology of $\mathcal{B}(V)$ is defined to be

$$H^i(\mathcal{B}(V), \mathbf{k}) := H^i(\Omega\mathcal{B}(V), \partial) = \text{Ker } \partial^i / \text{Im } \partial^{i-1}.$$

Lemma 1.5.1. *Let V^* be the dual of V in ${}^G\mathcal{YD}$. Suppose $\mathcal{B}(V)$ is finite-dimensional. Then $H^i(\mathcal{B}(V), \mathbf{k}) = \text{HH}^i(\mathcal{B}(V^*), \mathbf{k})$, where $\text{HH}^i(\mathcal{B}(V^*), \mathbf{k})$ is the i -th Hochschild cohomology of $\mathcal{B}(V^*)$ with coefficient in the trivial module \mathbf{k} .*

Proof. Note that $*V = V^*$ since $S^2 = \text{id}$ in $D(G)$. According to [1, 3.2.30], one sees that $\mathcal{B}(V)^{*bop} \cong \mathcal{B}(V^*)$ as connected graded braided Hopf algebras in ${}^G\mathcal{YD}$. Hence,

by [22, Proposition 1.4], we have

$$H^i(\mathcal{B}(V), \mathbf{k}) = HH^i(\mathcal{B}(V)^*, \mathbf{k}) = HH^i(\mathcal{B}(V)^{*bop}, \mathbf{k}) = HH^i(\mathcal{B}(V^*), \mathbf{k}).$$

□

It is important to point out that there is a bigrading structure on the Hochschild cohomology of $\mathcal{B}(V)$, that is, the homological grading and the Adams grading induced from the grading of $\mathcal{B}(V)$. From now on, we write

$$H^i(\mathcal{B}(V), \mathbf{k}) = \bigoplus_{j \geq 0} H^{i,j}(\mathcal{B}(V), \mathbf{k}),$$

where $H^{i,j}(\mathcal{B}(V), \mathbf{k})$ is the direct summand of $H^i(\mathcal{B}(V), \mathbf{k})$ in ${}^G\mathcal{YD}$ consisting of homogeneous elements whose Adams grading is j . Moreover, we have

Lemma 1.5.2. *The Hochschild cohomology ring $\bigoplus_{i,j \geq 0} H^{i,j}(\mathcal{B}(V), \mathbf{k})$ is a bigraded braided algebra in ${}^G\mathcal{YD}$.*

Proof. The braided algebra structure can be computed from the cobar construction $\Omega\mathcal{B}(V) = T(\mathcal{B}(V)^+)$. One sees that $T(\mathcal{B}(V)^+)$ is a bigraded braided algebra in ${}^G\mathcal{YD}$ with the tensor degree (inducing the homological grading) and the inner degree of $\mathcal{B}(V)$ (inducing the Adams grading). One can check that all the differentials are module maps in ${}^G\mathcal{YD}$ since they are constructed from the comultiplication of $\mathcal{B}(V)$. Moreover, the differentials also preserve the bigrading of $\Omega\mathcal{B}(V)$. Hence, the result follows after taking cohomology. □

Theorem 1.5.3. *Let $R = \bigoplus_{i \geq 0} R_i$ be a connected, coradically graded, and braided Hopf algebra in ${}^G\mathcal{YD}$. Suppose R is not primitively generated. Then the differential ∂^1 induces an injective Yetter-Drinfeld module map*

$$\partial^1 : R_d/\mathcal{B}(R_1)_d \hookrightarrow H^{2,d}(\mathcal{B}(R_1), \mathbf{k}),$$

where $d \geq 2$ is the smallest integer such that $\mathcal{B}(R_1)_d \subsetneq R_d$.

Proof. By the definition of Nichols algebra, $\mathcal{B}(R_1)$ is a graded Hopf subalgebra of R . Moreover, since R is coradically graded, $\mathcal{B}(R_1)$ contains all primitive elements R_1 of R . Note that the integer $d \geq 2$ is well-defined for R is not primitively generated.

First, we show that ∂^1 is well-defined on $R_d/\mathcal{B}(R_1)_d$. Choose any $z \in R_d$. Without loss of generality, we can assume $z \in R_{\geq 1}$ and write

$$\Delta(z) = z \otimes 1 + 1 \otimes z + \omega,$$

where $\omega \in \bigoplus_{j=1}^{d-1} R_j \otimes R_{d-j}$ since R is a graded coalgebra. By the choice of d , $R_j \otimes R_{d-j} \subseteq \mathcal{B}(R_1) \otimes \mathcal{B}(R_1)$ for all $1 \leq j \leq d-1$. Therefore, $\omega \in \mathcal{B}(R_1) \otimes \mathcal{B}(R_1)$. Moreover, the coalgebra structure of R is coassociative, so $(\Delta \otimes \text{id})\Delta = (\text{id} \otimes \Delta)\Delta$ on z . Thus, we have:

$$\begin{aligned} (\Delta \otimes \text{id})(z \otimes 1 + 1 \otimes z + \omega) &= \Delta(z) \otimes 1 + 1 \otimes 1 \otimes z + (\Delta \otimes \text{id})(\omega) \\ &= (z \otimes 1 + 1 \otimes z + \omega) \otimes 1 + 1 \otimes 1 \otimes z + (\Delta \otimes \text{id})(\omega); \\ (\text{id} \otimes \Delta)(z \otimes 1 + 1 \otimes z + \omega) &= z \otimes 1 \otimes 1 + 1 \otimes \Delta(z) + (\text{id} \otimes \Delta)(\omega) \end{aligned}$$

$$= z \otimes 1 \otimes 1 + 1 \otimes (z \otimes 1 + 1 \otimes z + \omega) + (\text{id} \otimes \Delta)(\omega),$$

which implies $1 \otimes \omega - (\Delta \otimes \text{id})(\omega) + (\text{id} \otimes \Delta)(\omega) - \omega \otimes 1 = 0$, equivalent to saying $\partial^1(z) = \omega$ is a 2-cocycle in $\Omega\mathcal{B}(V)$. By the construction of ∂^1 , we can conclude that $\partial^1 : z \mapsto \omega$ induces a map from R_d to $H^{2,d}(\mathcal{B}(R_1), \mathbf{k})$, which is also a Yetter-Drinfeld module map and preserves the Adams grading of $\mathcal{B}(V)$. Furthermore, the map ∂^1 factors through the Yetter-Drinfeld submodule $B(R_1)_d$ since $\partial^2 \partial^1 = 0$ in $\Omega\mathcal{B}(R_1)$.

Next we show that ∂^1 is injective after the factorization. Suppose $\partial^1(z) = \omega = \partial^1(x)$, for some $x \in \mathcal{B}(R_1)^+$. Then we have $\Delta(z) - z \otimes 1 - 1 \otimes z = \omega = \Delta(x) - x \otimes 1 - 1 \otimes x$. Hence $\Delta(z - x) = (z - x) \otimes 1 + 1 \otimes (z - x)$, so $(z - x)$ is a primitive element in R and it belongs to $R_1 \subset \mathcal{B}(R_1)^+$. So $z = x + (z - x) \in \mathcal{B}(R_1)^+$, which yields that $z \in \mathcal{B}(R_1) \cap R_d = \mathcal{B}(R_1)_d$. This proves the theorem. \square

Therefore, the second Hochschild cohomology group $H^2(\mathcal{B}(R_1), \mathbf{k})$ controls the non-primitive generators, if any, of a connected coradically graded braided Hopf algebra R in ${}^G\mathcal{YD}$. We obtain the following result.

Corollary 1.5.4. *Let R be as stated as in 1.5.3. If $H^2(\mathcal{B}(R_1), \mathbf{k}) = 0$, then $\mathcal{B}(R_1) = R$. As a consequence, if R is not primitively generated, then $H^2(\mathcal{B}(R_1), \mathbf{k})$ does not vanish.*

Since $H^n(\Omega\mathcal{B}(V))$ is a Yetter-Drinfeld module over $\mathbf{k}G$, we denote by $H^n(\Omega\mathcal{B}(V))^{coG}$ the coinvariants of $\mathbf{k}G$ in $H^n(\Omega\mathcal{B}(V))$, that is the trivial G -grading part. Note that $\bigoplus_{n \geq 0} H^n(\Omega\mathcal{B}(V))^{coG}$ is a subalgebra of $\bigoplus_{n \geq 0} H^n(\Omega\mathcal{B}(V))$.

Proposition 1.5.5. *Suppose $\mathcal{B}(V)$ is finite-dimensional. Then $H^n(\Omega(\mathcal{B}(V) \# \mathbf{k}G)) = H^n(\Omega\mathcal{B}(V))^{coG}$, for all $n \geq 0$. As a consequence,*

$$\bigoplus_{n \geq 0} H^n(\Omega(\mathcal{B}(V) \# \mathbf{k}G)) \cong \bigoplus_{n \geq 0} H^n(\Omega\mathcal{B}(V))^{coG}$$

as algebras.

Proof. By [1, §2.2], we know $B(V)^*$ is a braided Hopf algebra over $(\mathbf{k}G)^*$, and $(\mathcal{B}(V) \# \mathbf{k}G)^* \cong \mathcal{B}(V)^* \# (\mathbf{k}G)^*$ as Hopf algebras. There is a well-known spectral sequence of algebras, for example see reference [21],

$$HH^p((\mathbf{k}G)^*, HH^q(\mathcal{B}(V)^*, \mathbf{k})) \implies HH^{p+q}(\mathcal{B}(V)^* \# (\mathbf{k}G)^*, \mathbf{k}).$$

Since $(\mathbf{k}G)^*$ is semisimple, we have

$$HH^q(\mathcal{B}(V)^*, \mathbf{k})^{(\mathbf{k}G)^*} \cong HH^q(\mathcal{B}(V)^* \# (\mathbf{k}G)^*, \mathbf{k})$$

as algebras. Therefore, by the same argument in Lemma 1.5.1, we get

$$\begin{aligned} H^n(\Omega(\mathcal{B}(V) \# \mathbf{k}G)) &\cong HH^n((\mathcal{B}(V) \# \mathbf{k}G)^*, \mathbf{k}) \\ &\cong HH^n(\mathcal{B}(V)^* \# (\mathbf{k}G)^*, \mathbf{k}) \\ &\cong HH^n(\mathcal{B}(V)^*, \mathbf{k})^{(\mathbf{k}G)^*} \\ &\cong H^n(\Omega\mathcal{B}(V))^{coG}. \end{aligned}$$

\square

2. NICHOLS ALGEBRAS OF INFINITESIMAL BRAIDINGS OF RANK TWO

2.1. Indecomposable 2-dimensional ${}^G\mathcal{YD}$ modules. In this section, we work over an algebraically closed field \mathbf{k} of any characteristic. Let G be a finite group.

There are two different ways to construct a two-dimensional Yetter-Drinfeld module V over G . One is to choose a pair $(\varphi, g) \in \text{rep}_2(G) \times Z(G)$. Then V is constructed as a two-dimensional Yetter-Drinfeld module over G , where the G -action on V is given by $\varphi : G \rightarrow GL_2(V)$ and V has constant G -grading given by g . On the other hand, let $g \in G$ such that the centralizer $C(g)$ is of index two in G . Then for any character $\chi : C(g) \rightarrow \mathbf{k}$, take $V = \mathbf{k}G \otimes_{C(g)} \chi$, where the G -action is the induced action on χ and the G -coaction on $x \otimes \chi$, for any $x \in G$, is given by xgx^{-1} . In both constructions, we denote by $V = (\varphi, g) \in \text{rep}_2(G) \times Z(G)$ or $V = (\chi, g) \in \widehat{C(g)} \times G$.

Lemma 2.1.1. *Suppose $V \in {}^G\mathcal{YD}$ is indecomposable of dimension 2, then V is isomorphic to one of the following:*

- (1) $V = (\varphi, g) \in \text{rep}_2(G) \times Z(G)$, where φ is a two-dimensional indecomposable representation of $\mathbf{k}G$.
- (2) $V = (\chi, g) \in \widehat{C(g)} \times G$, where $C(g)$ has index two in G .

Proof. By Corollary 1.3.4 and the discussion below it, any indecomposable Yetter-Drinfeld module over G is given in terms of $V = \mathbf{k}G \otimes_{C(g)} M$, where M is an indecomposable module over $C(g)$. Suppose $\dim V = 2$. Then either $\dim M = 2$, in this case $C(g) = G$ so g is central; or $\dim M = 1$ and $|G : C(g)| = 2$. The result follows. \square

In the following, we denote by \mathcal{M}_G^2 the isomorphism classes of all two-dimensional indecomposable modules over $\mathbf{k}G$. Note that when $\mathbf{k} = \overline{\mathbf{k}}$ and $\text{char } \mathbf{k} \nmid |G|$, \mathcal{M}_G^2 contains all the 2×2 matrix blocks of the semisimple algebra $\mathbf{k}G$. In the conjugacy class decomposition $G = \sqcup_{1 \leq i \leq n} \mathcal{O}_i$, for any $g_i \in \mathcal{O}_i$, $\widehat{C(g_i)}$ denotes all the characters on the centralizer $C(g_i)$. Note that $\widehat{C(g_i)}$ is bijective to the set of grouplike elements in the dual Hopf algebra $\mathbf{k}^{C(g_i)}$. The next result is straightforward from previous argument.

Proposition 2.1.2. *The set of isomorphism classes of two-dimensional indecomposable Yetter-Drinfeld modules over G is bijective to the following set:*

$$(\mathcal{M}_G^2 \times Z(G)) \bigsqcup \left(\sqcup_{|\mathcal{O}_i|=2} \widehat{C(g_i)} \right).$$

2.2. Infinitesimal braidings of 2-dimensional ${}^G\mathcal{YD}$ modules. We discuss infinitesimal braidings of a two-dimensional Yetter-Drinfeld module V over G . Let \mathcal{O}_i be an orbit in the conjugacy class decomposition $G = \sqcup_{1 \leq i \leq n} \mathcal{O}_i$ satisfying $|\mathcal{O}_i| = 2$. For any $g \in \mathcal{O}_i$ and any character $\chi : C(g) \rightarrow \mathbf{k}$, we can construct a two-dimensional indecomposable Yetter-Drinfeld module $\mathbf{k}G \otimes_{C(g)} \chi$ over G . We denote it by $V = (\chi, g)$.

Lemma 2.2.1. *Suppose $V = (\chi, g) \in \widehat{C(g)} \times G$, where $C(g)$ has index two in G . Then V is of diagonal type with braiding matrix $(\chi(g))_{2 \times 2}$.*

Proof. Since $|G : C(g)| = 2$, there exists an element $s \in G \setminus C(g)$ such that $G = C(g) \sqcup C(g)s = C(g) \sqcup sC(g)$. Therefore $V = \mathbf{k}G \otimes_{C(g)} \chi$ has a basis $x_1 = 1_G \otimes \chi$ and $x_2 = s \otimes \chi$. Regarding the G -coaction on V , one sees that

$$\rho(x_1) = 1_G g 1_G^{-1} \otimes (1_G \otimes \chi) = g \otimes x_1, \quad \rho(x_2) = s g s^{-1} \otimes (s \otimes \chi) = s g s^{-1} \otimes x_2.$$

The G -action on x_1 is given by

$$h \cdot x_1 = h \cdot (1_G \otimes \chi) = 1_G \otimes h \cdot \chi = \chi(h)(1_G \otimes \chi) = \chi(h)x_1, \text{ for any } h \in C(g); \text{ and} \\ s \cdot x_1 = s \cdot (1_G \otimes \chi) = s \otimes \chi = x_2.$$

And G acts on x_2 via

$$h \cdot x_2 = h \cdot (s \otimes \chi) = s \otimes h' \cdot \chi = \chi(h')(s \otimes \chi) = \chi(h')x_2 = \chi(h)x_2, \text{ for any } h \in C(g), \\ \text{where } hs = sh' \text{ for some } h' \in G \text{ and } \chi(h) = \chi(h'); \text{ and}$$

$$s \cdot x_2 = s \cdot (s \otimes \chi) = s^2 \cdot (1_G \otimes \chi) = 1_G \otimes s^2 \cdot \chi = \chi(s^2)(1_G \otimes \chi) = \chi(s^2)x_1,$$

since $s^2 \in C(g)$. In particular, we have

$$s g s^{-1} \cdot x_1 = \chi(h g h^{-1})x_1 = \chi(g)x_1,$$

since $s g s^{-1} \in C(g)$; and

$$s g s^{-1} \cdot x_2 = s g s^{-1} \cdot (s \otimes \chi) = s g \cdot (1_G \otimes \chi) = s g \cdot x_1 = \chi(g)s \cdot x_1 = \chi(g)x_2.$$

Hence, we see that V is of diagonal type and the braiding matrix is $\mathfrak{q} = (\chi(g))_{2 \times 2}$. \square

Proposition 2.2.2. *Let V be a two-dimensional Yetter-Drinfeld module over G . Then the infinitesimal braiding of V is either of diagonal type or of Jordan type. Moreover, we have*

- (1) *If V is decomposable, then V is of diagonal type.*
- (2) *If $V = (\varphi, g) \in \text{rep}_2(G) \times Z(G)$, then V is of diagonal type provided $\varphi(g)$ is diagonalizable on V , otherwise V is of Jordan type.*
- (3) *If $V = (\chi, g) \in \widehat{C(g)} \times G$, then V is of diagonal type.*

Proof. (1) Suppose V is decomposable. Then $V = V_1 \oplus V_2$, where each V_i is a one-dimensional ${}^G_G\mathcal{YD}$ module. So V is of diagonal type by Proposition 1.4.1.

(2) Suppose $V = (\varphi, g) \in \text{rep}_2(G) \times Z(G)$, where $\varphi : G \rightarrow \text{GL}(V)$ is a two-dimensional representation of G . Clearly, V can be viewed as a Yetter-Drinfeld module over the subgroup $\langle g \rangle$ of G . We use the fact that $\dim V = 2$. If $\varphi(g)$ is diagonalizable on V , then $V = V_1 \oplus V_2$, where each V_i is a one-dimensional Yetter-Drinfeld module over $\langle g \rangle$. Hence, by Proposition 1.4.1, V is of diagonal type. Otherwise, the minimal polynomial of $\varphi(g)$ must be $(g - t)^2 = 0$ on V , for some $t \in \mathbf{k}^\times$. Then it again follows from Proposition 1.4.1 that V is of Jordan type.

(3) comes from Lemma 2.2.1.

Now according to Lemma 2.1.1, we conclude that V is either of diagonal type or of Jordan type. \square

2.3. Nichols algebras of infinitesimal braidings in positive characteristic.

In the remaining of our paper, let \mathbf{k} be an algebraically closed field of characteristic $p > 0$. We use the convention $(x)(\text{ad } y) := [x, y]$ (resp. $(\text{ad } y)(x) := [y, x]$) for the right (resp. left) adjoint action. The following proposition is used frequently in positive characteristic.

Proposition 2.3.1. [10, pp. 186-187] *Let A be any associative \mathbf{k} -algebra over a field of characteristic $p > 0$. For any $x, y \in A$, we have*

$$(x + y)^p = x^p + y^p + \sum_{i=1}^{p-1} s_i(x, y)$$

where $s_i(x, y)$ is the coefficient of λ^{i-1} in $x(\text{ad } (\lambda x + y))^{p-1}$, and

$$[x, y^p] = (x)(\text{ad } y)^p.$$

Let G be a finite p -group. We are interested in Nichols algebras $\mathcal{B}(V)$ for any two-dimensional Yetter-Drinfeld module V over $\mathbf{k}G$. Our next result is a restatement of 2.2.2 in characteristic $p > 0$.

Lemma 2.3.2. *Let G be a finite p -group and V be a two-dimensional Yetter-Drinfeld module over G . By choosing a suitable basis $\{x_1, x_2\}$ for V , we have:*

- (1) *If V is decomposable, then $V = (g_1, g_2, \varepsilon)$, where G coacts on x_i by some $g_i \in G$ and the G -action is trivial.*
- (2) *If $V = (\varphi, g) \in \text{rep}_2(G) \times Z(G)$, then either g acts trivially or $g \cdot x_1 = x_1$, $g \cdot x_2 = x_2 + x_1$.*
- (3) *If $p = 2$ and $V = (\varepsilon, g) \in \widehat{C(g)} \times G$ with $|G : C(g)| = 2$, then, for some $s \in G \setminus C(g)$, G coacts on x_1 by g and coacts on x_2 by sgs^{-1} ; and the $C(g)$ -action is trivial and $s \cdot x_1 = x_2$, $s \cdot x_2 = x_1$.*

Proof. Note that for G (or any subgroup of G) we only have the trivial character $\varepsilon : G \rightarrow \mathbf{k}$. Moreover, since G is a finite p -group and $\text{char. } \mathbf{k} = p > 0$, we have $g^{|G|} - 1 = (g - 1)^{|G|} = 0$. Hence in the Jordan type, the minimal polynomial for g is given by $(g - 1)^2 = 1$. Also note that case (3) only happens in $p = 2$ since $2 \mid |G|$. Then we can apply Lemma 2.2.1 and Proposition 2.2.2. \square

Next we focus on two-dimensional Yetter-Drinfeld modules V of *Jordan type*. By Lemma 2.3.2, there is a basis x_1, x_2 for V and a central group element $g \in Z(G)$ such that

$$g \cdot x_1 = x_1, \quad g \cdot x_2 = x_2 + x_1;$$

and both x_i have the same G -grading given by g . We denote by $\mathbf{k}\langle V \rangle$ the free braided Hopf algebra in ${}^G_G\mathcal{YD}$ generated by V , where x_1, x_2 are primitive elements. It is easy for one to check that x_1^p is primitive in $\mathbf{k}\langle V \rangle$, i.e., $\Delta(x_1^p) = 1 \otimes x_1^p + x_1^p \otimes 1$.

Lemma 2.3.3. *Suppose $p > 2$. In the braided Hopf algebra $\mathbf{k}\langle V \rangle$, we have $x_1 x_2 - \frac{1}{2} x_1^2$ is primitive. Moreover when we pass to the quotient braided Hopf algebra $\mathbf{k}\langle V \rangle / (x_1^p, x_1 x_2 - x_2 x_1 - \frac{1}{2} x_1^2)$, x_2^p is primitive.*

Proof. Clearly, we have

$$\begin{aligned}
& \Delta(x_1x_2 - x_2x_1) \\
&= (x_1 \otimes 1 + 1 \otimes x_1)(x_2 \otimes 1 + 1 \otimes x_2) - (x_2 \otimes 1 + 1 \otimes x_2)(x_1 \otimes 1 + 1 \otimes x_1) \\
&= (x_1x_2 - x_2x_1) \otimes 1 + g \cdot x_2 \otimes x_1 - g \cdot x_1 \otimes x_2 + 1 \otimes (x_1x_2 - x_2x_1) \\
&= (x_1x_2 - x_2x_1) \otimes 1 + x_1 \otimes x_1 + 1 \otimes (x_1x_2 - x_2x_1).
\end{aligned}$$

Subtracting $\Delta(\frac{1}{2}x_1^2) = \frac{1}{2}x_1^2 \otimes 1 + x_1 \otimes x_1 + 1 \otimes \frac{1}{2}x_1^2$ from the above equation, we deduce that $x_1x_2 - x_2x_1 - \frac{1}{2}x_1^2$ is primitive.

Now consider the quotient braided Hopf algebra $A := \mathbf{k}\langle V \rangle / (x_1^p, x_1x_2 - x_2x_1 - \frac{1}{2}x_1^2)$. By induction on $n \geq 1$, we have

$$x_1^n x_2 - x_2 x_1^n = \frac{n}{2} x_1^{n+1}.$$

Next we prove the following identity inductively

$$(2.3.3.1) \quad (x_2 \otimes 1)(\text{ad}(\lambda x_2 \otimes 1 + 1 \otimes x_2))^n = -\frac{(n+1)!}{2^n} \lambda^{n-1} x_1^n \otimes x_2,$$

for all $n \geq 1$ in the braided algebra $A \otimes A$. First, one checks that it holds for $n = 1$:

$$\begin{aligned}
[x_2 \otimes 1, \lambda x_2 \otimes 1 + 1 \otimes x_2] &= \lambda x_2^2 \otimes 1 + x_2 \otimes x_2 - \lambda x_2^2 \otimes 1 - g \cdot x_2 \otimes x_2 \\
&= -x_1 \otimes x_2.
\end{aligned}$$

Suppose it is true for $n = m$. Then for $n = m + 1$, we have

$$\begin{aligned}
& (x_2 \otimes 1)(\text{ad}(\lambda x_2 \otimes 1 + 1 \otimes x_2))^{m+1} \\
&= [-\frac{(m+1)!}{2^m} \lambda^{m-1} x_1^m \otimes x_2, \lambda x_2 \otimes 1 + 1 \otimes x_2] \\
&= -\frac{(m+1)!}{2^m} \lambda^{m-1} [x_1^m \otimes x_2, \lambda x_2 \otimes 1 + 1 \otimes x_2] \\
&= -\frac{(m+1)!}{2^m} \lambda^{m-1} (\lambda x_1^m (g \cdot x_2) \otimes x_2 + x_1^m \otimes x_2^2 - \lambda x_2 x_1^m \otimes x_2 - g \cdot (x_1^m) \otimes x_2^2) \\
&= -\frac{(m+1)!}{2^m} \lambda^{m-1} (\lambda x_1^{m+1} \otimes x_2 + \lambda (x_1^m x_2 - x_2 x_1^m) \otimes x_2) \\
&= -\frac{(m+1)!}{2^m} \lambda^{m-1} \lambda (1 + \frac{m}{2}) x_1^{m+1} \otimes x_2 \\
&= -\frac{(m+2)!}{2^{m+1}} \lambda^m x_1^{m+1} \otimes x_2.
\end{aligned}$$

This proves (2.3.3.1). Now we apply Proposition 2.3.1. Then

$$\Delta(x_2^p) = (x_2 \otimes 1 + 1 \otimes x_2)^p = x_2^p \otimes 1 + 1 \otimes x_2^p + \sum_{i=1}^{p-1} s_i(x_2 \otimes 1, 1 \otimes x_2),$$

where $is_i(x_2 \otimes 1, 1 \otimes x_2)$ is the coefficient of λ^{i-1} in (2.3.3.1) by letting $n = p - 1$. One sees that all terms of λ^{i-1} vanish as $n = p - 1$. Hence x_2^p is primitive. \square

Proposition 2.3.4. *Let V be a two-dimensional Yetter-Drinfeld module over $\mathbf{k}G$ with basis $\{x_1, x_2\}$.*

- (1) *If V is of diagonal type, then $\mathcal{B}(V) = \mathbf{k}[x_1, x_2]/(x_1^p, x_2^p)$.*
- (2) *If V is of Jordan type, then*

$$\mathcal{B}(V) = \begin{cases} \mathbf{k}\langle x_1, x_2 \rangle / (x_1^2, x_2^4, x_2^2 x_1 + x_1 x_2^2 + x_1 x_2 x_1, x_1 x_2 x_1 x_2 + x_2 x_1 x_2 x_1), & p = 2 \\ \mathbf{k}\langle x_1, x_2 \rangle / (x_1^p, x_2^p, x_1 x_2 - x_2 x_1 - \frac{1}{2} x_1^2), & p > 2. \end{cases}$$

In both cases, $V = \text{Span}\{x_1, x_2\}$ is the primitive space of $\mathcal{B}(V)$.

Proof. (1) If V is of diagonal type, then it must have trivial braiding by Lemma 2.3.2. Following similar computation argument as in Lemma 2.3.3, we can check that x_1^p, x_2^p and $[x_1, x_2]$ are all primitive. Hence the Nichols algebra $\mathcal{B}(V)$ is given by $\mathbf{k}[x_1, x_2]/(x_1^p, x_2^p)$.

(2) The Jordan type can be derived from [9, Theorem 3.1 and Theorem 3.5]. Here we give a short proof for the case $p > 2$. By Lemma 2.3.3, one sees that $\mathcal{B}(V)$ is a braided Hopf algebra quotient of $B := \mathbf{k}\langle x_1, x_2 \rangle / (x_1^p, x_2^p, x_1 x_2 - x_2 x_1 - \frac{1}{2} x_1^2)$. Hence, it suffices to show that any braided Hopf ideal $0 \neq I \subset B$ must have $I \cap V \neq 0$. It is easy to check that $\dim B = p^2$. Since Nichols-Zoeller's freeness theorem [17] still holds for B , $(\dim B/I)$ must divide p^2 . Suppose $I \cap V = 0$. Then there would be embeddings for the two Hopf subalgebras $\mathbf{k}[x_1]$ and $\mathbf{k}[x_2]$ into B/I . This implies that $\dim B/I = p^2$ and $I = 0$. Hence we obtain a contradiction. By the definition of $\mathcal{B}(V)$, we have $\mathcal{B}(V) = B$. \square

We make a remark on $\dim \mathcal{B}(V)$ for the Jordan type in case (2) of Proposition 2.3.4. When $p = 2$, $\mathcal{B}(V)$ is a sixteen-dimensional algebra with basis

$$1, x_1, x_2, x_1 x_2, x_2 x_1, x_2^2, x_1 x_2 x_1, x_1 x_2^2, \\ x_2 x_1 x_2, x_2^3, x_1 x_2 x_1 x_2, x_1 x_2^3, x_2 x_1 x_2^2, x_1 x_2 x_1 x_2^2, x_2 x_1 x_2^3, x_1 x_2 x_1 x_2^3.$$

When $p > 2$, $\mathcal{B}(V)$ is of dimension p^2 with basis $\{x_1^i x_2^j \mid 0 \leq i, j \leq p-1\}$.

Corollary 2.3.5. *Let \mathbf{k} be an algebraically closed field of characteristic $p > 0$, and V be a Yetter-Drinfeld module over a finite p -group G . Then if $\dim V \leq 2$, we have $\dim \mathcal{B}(V) < \infty$.*

Proof. The case of $\dim V = 1$ is easy to check and the case of $\dim V = 2$ follows from Proposition 2.3.4. \square

3. POINTED p^3 -DIMENSIONAL HOPF ALGEBRAS: STRUCTURES OF R AND OF $\text{gr } H$

For the rest of the paper, we let our base field \mathbf{k} be algebraically closed of prime characteristic $p > 0$. Let H be any pointed Hopf algebra of dimension p^3 over \mathbf{k} with $H_0 = \mathbf{k}G = \mathbf{k}G(H)$. Our goal is to classify all isomorphism classes of such H . Our strategy is first to classify $\text{gr } H \cong R \# \mathbf{k}G$, where R is a graded braided Hopf algebra in ${}^G_G \mathcal{YD}$, then lift $\text{gr } H$ structures to H . As the dimension of H_0 divides the dimension of H by Nichols-Zoeller Theorem [17], we consider the following cases:

(a) If $\dim H_0 = 1$, then $H_0 = \mathbf{k}$, i.e., H is connected. This part was done by joint work of both authors with L. Wang in [15, 16].

(b) If $\dim H_0 = p$, then $G = C_p = \langle g \rangle$ and $\dim R = p^2$. This part is discussed in Section 3.1 cases (A)-(B) and in Section 3.2 case (C), where (C) is the non-primitively generated case.

(c) If $\dim H_0 = p^2$, then $G = C_{p^2}$ or $C_p \times C_p$ and $\dim R = p$. This part is handled in Section 3.1 case (D).

(d) If $\dim H_0 = p^3$, then $H = \mathbf{k}G$ is a group algebra of dimension p^3 . The classification of finite groups of order p^3 is well-known:

- **abelian:** $C_{p^3}, C_{p^2} \times C_p, C_p \times C_p \times C_p$.
- **non-abelian:** dihedral group D_4 and quaternion group Q_8 for $p = 2$; and for $p > 2$, Heisenberg group $UT(3, p)$ and

$$G_p = \left\{ \begin{pmatrix} 1 + \binom{p}{1} & b \\ 0 & 1 \end{pmatrix}, (p) = p\mathbb{Z}/(p^2), \text{ and } b \in \mathbb{Z}/(p^2) \right\}.$$

3.1. R is primitively generated. In this section, suppose that R is primitively generated, that is R is generated by $R_0 = \mathbf{k}$ and $R_1 = P(R)$ of primitive elements. In this case, we know $R = \mathcal{B}(R_1)$ Nichols algebra, which is uniquely determined by the infinitesimal braiding of R_1 .

If $H_0 = \mathbf{k}C_p$ with generator g of C_p , then R_1 is two-dimensional with basis $\{r_1, r_2\}$. The structure of $R \in {}^G\mathcal{YD}$ depends on how G (co)acts on these basis elements. We apply Lemma 2.3.2.

Case (A). $G = C_p = \langle g \rangle$ and R_1 is of diagonal type. Suppose $p > 2$, this forces the action of G to be trivial:

$$g \cdot r_1 = r_1, \quad g \cdot r_2 = r_2.$$

Assume r_1, r_2 have G -gradings g^u, g^v , respectively, for some $u, v \in \{0, 1, \dots, p-1\}$. Without loss of generality, we may obtain either

- **(A1):** The G -coaction is non-trivial. We can assume $\rho_R(r_1) = g \otimes r_1$ and $\rho_R(r_2) = g^u \otimes r_2$, for $0 \leq u \leq p-1$; or
- **(A2):** The G -coaction is trivial, that is $\rho_R(r_1) = 1 \otimes r_1$ and $\rho_R(r_2) = 1 \otimes r_2$.

Suppose $p = 2$, then the G -coaction is trivial and g interchanges r_1 and r_2 such that

- **(A3):** $g \cdot r_1 = r_2, g \cdot r_2 = r_1$, and $\rho_R(r_1) = 1 \otimes r_1, \rho_R(r_2) = 1 \otimes r_2$.

By Proposition 2.3.4, the structure of R is determined by $R = \mathbf{k}[r_1, r_2]/(r_1^p, r_2^p)$ in all three cases.

Case (B). $G = C_p = \langle g \rangle$ and R_1 is of Jordan type. This only happens when $p > 2$, since if $p = 2$ Proposition 2.3.4 shows that $\dim B(R_1) = 2^4 \neq 2^2$. We can assume r_1, r_2 have the same G -grading g with G -action

$$g \cdot r_1 = r_1 \quad g \cdot r_2 = r_1 + r_2.$$

By Proposition 2.3.4, the structure of R is determined by $R = \mathbf{k}\langle r_1, r_2 \rangle / (r_1^p, r_2^p, r_1 r_2 - r_2 r_1 - \frac{1}{2} r_1^2)$.

Case (D). $G = C_{p^2}$ or $C_p \times C_p$. Hence R_1 is one-dimensional with basis element r of some G -grading $g_u \in G$. Clearly G trivially acts on r .

If $G = C_{p^2}$, a cyclic group generated by g , then $g_u = g^s$ for some $s \geq 0$. There are three cases that can happen for this G -grading g^s :

- $s = 0$, hence $g^s = 1$;
- s is coprime with p^2 , then by changing generator, we can rewrite g^s as g ;
- $s = pv$, where v is coprime with p , then by changing generator, we can rewrite g^s as g^p .

It is clear that these three cases are not isomorphic.

If $G = C_p \times C_p = \langle g_1 \rangle \times \langle g_2 \rangle$, one can view G as a two-dimensional vector space over \mathbb{F}_p , picking a generator of G is the same as picking a basis of this vector space. Thus, having G -grading $g_u = (g_1, 1) \in G$ yields isomorphic result as having G -grading $g_u = (1, g_2)$.

Therefore, in case (D), without loss of generality, we can obtain either

- **(D1)**: When $G = C_{p^2} = \langle g \rangle$, we can take $g_u = 1$, g and g^p ; or
- **(D2)**: When $G = C_p \times C_p = \langle g_1 \rangle \times \langle g_2 \rangle$, we can take $g_u = 1$ or g_1 .

It is easy to see that R is determined by $R = \mathbf{k}[r]/(r^p)$.

3.2. R is non-primitively generated. In positive characteristic, R is not primitively generated in general. Thus, we need to consider an additional case:

Case (C). When $G = C_p = \langle g \rangle$ and assume R is generated by a primitive element $r \in R_1$ and a *non-primitive* element z . Then the only way G can act on primitive generator r is

$$g \cdot r = r, \quad \rho_R(r) = g^u \otimes r,$$

for some $u \in \{0, 1, \dots, p-1\}$. Without loss of generality, we can assume $g^u = 1$ or g ; and under this G -action, we have $r^p = 0$. Let $\mathcal{B}(R_1) = \mathbf{k}[r]/(r^p)$ be the Nichols algebra of R_1 . Then $\mathcal{B}(R_1)$ is a graded braided Hopf subalgebra of R of dimension p .

Claim: $\dim H^2(\mathcal{B}(R_1), \mathbf{k}) = 1$ and it is spanned by the 2-cocycle

$$(3.2.0.1) \quad \omega(r) := \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} (r^i \otimes r^{p-i}).$$

Proof of claim. Let R_1^* be the dual of R_1 in ${}^G\mathcal{YD}$. It is clear that R_1^* is still one-dimensional, hence it has trivial braiding since the G -action must be trivial. So one sees that $\mathcal{B}(R_1^*) \cong \mathbf{k}C_p$ as algebras. By Lemma 1.5.1, we have

$$\dim H^2(\mathcal{B}(R_1), \mathbf{k}) = \dim HH^2(\mathcal{B}(R_1^*), \mathbf{k}) = \dim HH^2(\mathbf{k}C_p, \mathbf{k}) = \dim H^2(C_p, \mathbf{k}) = 1.$$

It is easy to check that $\omega(r)$ is a 2-cocycle in the cobar construction $\Omega\mathcal{B}(R_1)$. By a similar degree argument as in [25, Proposition 6.2], one can conclude that $\omega(r)$ does not lie in the coboundary of $\Omega\mathcal{B}(R_1)$. \square

Observe that $\omega(r)$ has total degree (Adams grading) p in $\mathcal{B}(R_1)$ and $\mathcal{B}(R_1)_p = 0$. We apply 1.5.3 to get an injective Yetter-Drinfeld module map $\partial^1 : R_p \hookrightarrow \mathrm{HH}^{2p}(\mathcal{B}(R_1), \mathbf{k})$. By a simple dimension argument, one sees that ∂^1 is an isomorphism. Thus we can choose the non-primitive element z to be a basis of R_p and write

$$\Delta(z) = z \otimes 1 + 1 \otimes z + \omega(r).$$

Moreover, one checks that $\omega(r)$ has trivial G -grading since $g^{up} = 1$ by (3.2.0.1). Hence z also has trivial G -grading such that $\rho_R(z) = 1 \otimes z$.

To determine the relations between r and z , observe that the G -actions on them are both trivial. Hence

$$\begin{aligned} \Delta([r, z]) &= \Delta(rz - zr) = [r \otimes 1 + 1 \otimes r, z \otimes 1 + 1 \otimes z + \omega(r)] \\ &= (rz - zr) \otimes 1 + 1 \otimes (rz - zr) = [r, z] \otimes 1 + 1 \otimes [r, z]. \end{aligned}$$

So $[r, z] \in R_1 \cap R_{p+1} = 0$ and $rz = zr$. One can also easily compute $\Delta(z^p) = (z \otimes 1 + 1 \otimes z + \omega(r))^p = z^p \otimes 1 + 1 \otimes z^p + \omega(r^p) = z^p \otimes 1 + 1 \otimes z^p$, implying $z^p \in R_1 \cap R_{p^2} = 0$.

As a conclusion, for case (C), the structure of R is given by

$$R = \mathbf{k}[r, z]/(r^p, z^p),$$

where $r \in R_1$ is a primitive element of G -grading 1 or g , and $z \in R_p$ is a non-primitive element of trivial G -grading.

In summary, we obtain the following R -structures in $\mathrm{gr} H = R \# H_0$ in Table 1. Here, we use g to denote the generators of the cyclic groups C_p and C_{p^2} ; use g_1, g_2 to denote the generators of $C_p \times C_p$. The notation $\epsilon \in \{0, 1, p\}$ is used to mean $g^\epsilon = 1$ or g in C_p , and $g^\epsilon = 1, g$, or g^p in C_{p^2} .

3.3. Structure of $\mathrm{gr} H$. Given R and H_0 as classified in the previous section, here we will obtain their bosonization $\mathrm{gr} H \cong R \# H_0$. In the next section, we will lift the structures of $\mathrm{gr} H$ to H to classify pointed p^3 -dimensional Hopf algebras in positive characteristic $p > 0$.

Let us first set up some conventions. The underlying vector space structure of $\mathrm{gr} H \cong R \# H_0$ is $R \otimes H_0$. For all $g \in G$, we identify $g = 1 \# g \in \mathrm{gr} H$ via the inclusion ι . For cases (A1)-(A3) and (B), let $a := r_1 \# 1$ and $b := r_2 \# 1$. For case (C), let $a := r \# 1$ and $b := z \# 1$. For cases (D1)-(D2), let $a := r \# 1$.

We compute the structure of $\mathrm{gr} H$ using the structure formulas as seen in c.f. Section 1, [18], or [14, Theorem 10.6.5]. For cases (A1)-(A3), (B), and (D), when R is primitively generated, one can compute the bosonization structure of $\mathrm{gr} H \cong \mathcal{B}(V) \# \mathbf{k}G$ using simpler formulas, e.g. for all $g \in G$ and $v \in V = R_1$:

$$gv = (g \cdot v) \# g, \quad \text{and} \quad \Delta(v) = v \otimes 1 + v_{(-1)} \otimes v_{(0)}.$$

Since the computation is straightforward, we do not give details here. We obtain the following bosonization structures for $\mathrm{gr} H \cong R \# H_0$ in Table 2. It is a \mathbf{k} -algebra generated by $\{a, b, g\}$ in cases (A1)-(A3), (B), and (C); generated by $\{a, g\}$ in case (D1); and generated by $\{a, g_1, g_2\}$ in case (D2), where $C_p \times C_p = \langle g_1 \rangle \times \langle g_2 \rangle$. We also note that the Hopf algebras $\mathrm{gr} H$ of case (B) have appeared in [9].

TABLE 1. Structure of R – for pointed p^3 -dimensional Hopf algebras in characteristic $p > 0$, when $\dim H_0 = p$ or p^2

| Type of R | $G(H)$ | (Co)Alg. Structure of R | ${}^G\mathcal{YD}\text{-mod}$ Structure of R | # Iso. classes of R |
|---------------|------------------|--|--|-----------------------|
| (A1) | C_p | $r_1^p = r_2^p = 0, r_1 r_2 = r_2 r_1, \Delta(r_i) = r_i \otimes 1 + 1 \otimes r_i$ | $g \cdot r_i = r_i, \rho(r_1) = g \otimes r_1, \rho(r_2) = g^u \otimes r_2, 0 \leq u \leq p-1$ | p classes |
| (A2) | C_p | $r_1^p = r_2^p = 0, r_1 r_2 = r_2 r_1, \Delta(r_i) = r_i \otimes 1 + 1 \otimes r_i$ | $g \cdot r_i = r_i, \rho(r_i) = 1 \otimes r_i$ | one class |
| (A3) $p=2$ | C_p | $r_1^p = r_2^p = 0, r_1 r_2 = r_2 r_1, \Delta(r_i) = r_i \otimes 1 + 1 \otimes r_i$ | $g \cdot r_1 = r_2, g \cdot r_2 = r_1, \rho(r_i) = 1 \otimes r_i$ | one class |
| (B) $p>2$ | C_p | $r_1^p = r_2^p = 0, r_1 r_2 - r_2 r_1 = \frac{1}{2} r_1^2, \Delta(r_i) = r_i \otimes 1 + 1 \otimes r_i$ | $g \cdot r_1 = r_1, g \cdot r_2 = r_2 + r_1, \rho(r_i) = g \otimes r_i$ | one class |
| (C) | C_p | $r^p = z^p = 0, r z = z r, \Delta(r) = r \otimes 1 + 1 \otimes r, \Delta(z) = z \otimes 1 + 1 \otimes z + \omega(r)$ | $g \cdot r = r, g \cdot z = z, \rho(r) = g^\epsilon \otimes r, \rho(z) = 1 \otimes z$ | two classes |
| (D1) | C_{p^2} | $r^p = 0, \Delta(r) = r \otimes 1 + 1 \otimes r$ | $g \cdot r = r, \rho(r) = g^\epsilon \otimes r$ | three classes |
| (D2) | $C_p \times C_p$ | $r^p = 0, \Delta(r) = 1 \otimes r + r \otimes 1$ | $g_i \cdot r = r, \rho(r) = g_1^\epsilon \otimes r$ | two classes |

4. POINTED p^3 -DIMENSIONAL HOPF ALGEBRAS: LIFTINGS FROM $\text{gr } H$ TO H

We will now lift the structures of $\text{gr } H$, as seen in Table 2, to H . To do that, we need the following two lemmas:

Lemma 4.0.1. *Let G be a finite p -group and $\delta : \mathbf{k}G \rightarrow \mathbf{k}G$ be a \mathbf{k} -derivation on $\mathbf{k}G$. Then*

- (1) *Suppose $G = \langle g \rangle$ is cyclic of order $p^n =: q$ and $\delta(g) = g - g^2$. Then $\delta^m(g) = \sum_{0 \leq i \leq q-1} a_i^m g^i$, for $m \geq 1$, where the coefficients are defined by*

$$a_0^m = \sum_{1 \leq j \leq q-1} (-1)^j \binom{q-1}{j} j^m, \quad a_i^m = \sum_{0 \leq j \leq i-1} (-1)^j \binom{i-1}{j} (j+1)^m,$$

for $1 \leq i \leq q-1$. In particular, we have $\delta^p = \delta$ and $\delta^{p-1}(g) = g - g^p$.

- (2) *Suppose $G = \langle g \rangle$ is cyclic of order p and $\delta(g) = g - g^2$. For any integer $1 \leq u \leq p-1$, we have*

$$\left(\frac{\delta}{u} + \frac{\delta^2}{u^2} + \cdots + \frac{\delta^{p-1}}{u^{p-1}} \right) (g^{1+u}) = 0.$$

- (3) *Suppose $G = C_p$ is cyclic of order p and $\delta(g) = g - g^{u+1}$, for any $0 \leq u \leq p-1$. Then we have $\delta^p = \delta$.*
- (4) *Suppose $G = C_p \times C_p = \langle g \rangle \times \langle h \rangle$ and $\delta(g) = g - g^2, \delta(h) = \tau h(1 - g)$, for some $\tau \in \mathbf{k}$. Then $\delta^p = \delta$.*

TABLE 2. Structure of $\text{gr } H$ – for pointed p^3 -dimensional Hopf algebras in characteristic $p > 0$, when $\dim H_0 = p$ or p^2

| Type of R | $G(H)$ | Algebra Structure of $\text{gr } H$ | Hopf Structure of $\text{gr } H$ | # Iso. classes of $\text{gr } H$ |
|-----------------|------------------|--|--|----------------------------------|
| (A1) | C_p | $a^p = b^p = 0, g^p = 1, ab = ba, ga = ag, gb = bg$ | $\Delta(g) = g \otimes g, \Delta(a) = a \otimes 1 + g \otimes a, \Delta(b) = b \otimes 1 + g^u \otimes b, \varepsilon(g) = 1, \varepsilon(a) = \varepsilon(b) = 0, S(g) = g^{-1}, S(a) = -ag^{-1}, S(b) = -bg^{-u}, 0 \leq u \leq p-1$ | p classes |
| (A2) | C_p | $a^p = b^p = 0, g^p = 1, ab = ba, ga = ag, gb = bg$ | $\Delta(g) = g \otimes g, \Delta(a) = a \otimes 1 + 1 \otimes a, \Delta(b) = b \otimes 1 + 1 \otimes b, \varepsilon(g) = 1, \varepsilon(a) = \varepsilon(b) = 0, S(g) = g^{-1}, S(a) = -a, S(b) = -b$ | one class |
| (A3) $p = 2$ | C_p | $a^p = b^p = 0, g^p = 1, ab = ba, ga = bg, gb = ag$ | $\Delta(g) = g \otimes g, \Delta(a) = a \otimes 1 + 1 \otimes a, \Delta(b) = b \otimes 1 + 1 \otimes b, \varepsilon(g) = 1, \varepsilon(a) = \varepsilon(b) = 0, S(g) = g^{-1}, S(a) = -a, S(b) = -b$ | one class |
| (B) $p > 2$ | C_p | $a^p = b^p = 0, g^p = 1, ab = ba = \frac{1}{2}a^2, ga = ag, gb = (a+b)g$ | $\Delta(g) = g \otimes g, \Delta(a) = a \otimes 1 + g \otimes a, \Delta(b) = b \otimes 1 + g \otimes b, \varepsilon(g) = 1, \varepsilon(a) = \varepsilon(b) = 0, S(g) = g^{-1}, S(a) = -ag^{-1}, S(b) = (a-b)g^{-1}$ | one class |
| (C) | C_p | $a^p = b^p = 0, g^p = 1, ab = ba, ga = ag, gb = bg$ | $\Delta(g) = g \otimes g, \Delta(a) = a \otimes 1 + g^\epsilon \otimes a, \Delta(b) = b \otimes 1 + 1 \otimes b + \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} (a^i g^{\epsilon(p-i)} \otimes a^{p-i}), \varepsilon(g) = 1, \varepsilon(a) = \varepsilon(b) = 0, S(g) = g^{-1}, S(a) = -ag^{-\epsilon}, S(b) = -b$ | two classes |
| (D1) | C_{p^2} | $a^p = 0, g^{p^2} = 1, ga = ag$ | $\Delta(g) = g \otimes g, \Delta(a) = a \otimes 1 + g^\epsilon \otimes a, \varepsilon(g) = 1, \varepsilon(a) = 0, S(g) = g^{-1}, S(a) = -ag^{-\epsilon}$ | three classes |
| (D2) | $C_p \times C_p$ | $a^p = 0, g_1^p = g_2^p = 1, g_i a = a g_i$ | $\Delta(g_i) = g_i \otimes g_i, \Delta(a) = a \otimes 1 + g_1^\epsilon \otimes a, \varepsilon(g_i) = 1, \varepsilon(a) = 0, S(g_i) = g_i^{-1}, S(a) = -ag_1^{-\epsilon}$ | two classes |

Proof of Lemma 4.0.1. (1) We consider the matrix M of the \mathbf{k} -linear map δ under the basis $\{1 = g^0, g, g^2, \dots, g^{q-1}\}$ of $\mathbf{k}G$, where we associate each g^i to a standard column vector $e_i = [0, \dots, 0, 1, 0, \dots, 0]^T$, with the $(i+1)$ -th entry is 1 and zero everywhere else.

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & -(q-1) \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & -2 & 3 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -(q-3) & (q-2) & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & -(q-2) & (q-1) \end{pmatrix}_{q \times q}.$$

The matrix M can be diagonalized as

$$PMP^{-1} = \begin{pmatrix} 0 & & & & \\ & 1 & & & \\ & & 2 & & \\ & & & \ddots & \\ & & & & (q-1) \end{pmatrix}_{q \times q} =: D, \text{ by}$$

$$P = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & -2 & 1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 3 & -3 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & -\binom{q-3}{1} & \binom{q-3}{2} & -\binom{q-3}{3} & \dots & 1 & 0 \\ 0 & -1 & \binom{q-2}{1} & -\binom{q-2}{2} & \binom{q-2}{3} & \dots & -\binom{q-2}{q-3} & 1 \end{pmatrix}_{q \times q} \quad \text{and}$$

$$P^{-1} = \begin{pmatrix} 1 & -\binom{q-1}{1} & -\binom{q-1}{2} & -\binom{q-1}{3} & -\binom{q-1}{4} & \dots & -\binom{q-1}{q-2} & -1 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 3 & 3 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \binom{q-3}{1} & \binom{q-3}{2} & \binom{q-3}{3} & \dots & 1 & 0 \\ 0 & 1 & \binom{q-2}{1} & \binom{q-2}{2} & \binom{q-2}{3} & \dots & \binom{q-2}{q-3} & 1 \end{pmatrix}_{q \times q}.$$

Therefore, applying on $g = e_1$, we have:

$$\begin{aligned} \delta^m(g) &= M^m(e_1) = (P^{-1}DP)^m(e_1) = P^{-1}D^mP(e_1) \\ &= P^{-1}D^m[1, 1, -1, \dots, 1, -1]^T \\ &= P^{-1}[0, 1^m, -2^m, \dots, (q-2)^m, -(q-1)^m]^T \\ &= \sum_{0 \leq i \leq q-1} a_i^m e_i. \end{aligned}$$

Then it is easy to find the formulas for all the coefficients a_i^m . Moreover, we have $\delta^p = M^p = (P^{-1}DP)^p = P^{-1}D^pP = P^{-1}DP = M = \delta$. For δ^{p-1} , by the definition of δ , one sees that $a_i^{p-1} = 0$, for all $i > p$. If $q = p$, then it is easy to check that $a_0^{p-1} = -1$, $a_1^{p-1} = 1$ and $a_i^{p-1} = 0$, for $2 \leq i \leq p-1$. Hence $\delta^{p-1}(g) = g - 1 = g - g^p$. The argument for $q > p$ is similar.

(2) By the proof of (1), there are eigenvectors v_0, v_1, \dots, v_{p-1} in $\mathbf{k}G$ such that $\delta(v_i) = iv_i$, for $0 \leq i \leq p-1$. Then one sees that

$$\begin{aligned} \left(\frac{\delta}{u} + \left(\frac{\delta}{u} \right)^2 + \dots + \left(\frac{\delta}{u} \right)^{p-1} \right) (v_j) &= \left(\prod_{2 \leq i \leq p} \left(\frac{\delta}{u} - i \right) \right) (v_j) = \left(\prod_{2 \leq i \leq p} \left(\frac{j}{u} - i \right) \right) (v_j) \\ &= \begin{cases} 0, & j \neq u \\ \left(\prod_{2 \leq i \leq p} (1 - i) \right) (v_j) = (p-1)! (v_j), & j = u \end{cases} \end{aligned}$$

Moreover, by using the matrix P^{-1} , $v_i = P^{-1}(e_i)$. Hence

$$g^{1+u} = e_{1+u} = \begin{cases} \sum_{0 \leq i \leq p-1} v_i P_{i+1, u+2} = v_0 + \sum_{u \leq i \leq p-2} (-1)^{i-u} \binom{i}{u} v_{i+1}, & 1 \leq u \leq p-2 \\ v_0, & u = p-1 \end{cases}$$

So when we write g^{1+u} as a linear combination of v_i 's, it does not contain the linear term v_u . Thus $(\delta/u + \delta^2/u^2 + \dots + \delta^{p-1}/u^{p-1})(g^{1+u}) = 0$.

(3) As in the proof of (1), we consider the matrix M of the \mathbf{k} -linear map δ under the basis $\{1, g, g^2, \dots, g^{p-1}\}$. One sees that M is diagonalizable with eigenvalues $0, 1, 2, \dots, p-1$. Hence $\delta^p = \delta$.

(4) We put an ordering on the the basis $\{g^i h^j \mid 0 \leq i, j \leq p-1\}$ of $\mathbf{k}G$ such that $g^{i_1} h^{j_1} < g^{i_2} h^{j_2}$ whenever $(j_1 < j_2)$ or $(i_1 < i_2 \text{ if } j_1 = j_2)$. Then we consider the matrix M of the \mathbf{k} -linear map δ under the ordered basis $\{g^i h^j \mid 0 \leq i, j \leq p-1\}$. Since $\delta(g^i h^j) = (j\tau + i)g^i h^j - (j\tau + i)g^{i+1} h^j$, $M = \text{Diag}(B_0, B_1, \dots, B_{p-1})$ is a block matrix such that

$$\begin{aligned} B_0 &= \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & -(p-1) \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & -2 & 3 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -(p-3) & (p-2) & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & -(p-2) & (p-1) \end{pmatrix}_{p \times p} \quad \text{and} \\ B_j &= \begin{pmatrix} j\tau & 0 & 0 & 0 & \dots & 0 & -j\tau - (p-1) \\ -j\tau & j\tau + 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & -j\tau - 1 & j\tau + 2 & 0 & \dots & 0 & 0 \\ 0 & 0 & -j\tau - 2 & j\tau + 3 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & j\tau + (p-2) & 0 \\ 0 & 0 & 0 & 0 & \dots & -j\tau - (p-2) & j\tau + (p-1) \end{pmatrix}_{p \times p}, \end{aligned}$$

for $1 \leq j \leq p-1$. It suffices to show that each block B_j has eigenvalues $0, 1, \dots, p-1$, (mod p). Then, since B_j has size $p \times p$, it is diagonalizable and $B_j^p = B_j$. So $M^p = M$, which implies that $\delta^p = \delta$. From the proof of (1), this is true for B_0 ($p = q$). For B_j

($1 \leq j \leq p-1$), one can compute its characteristic polynomial as follows

$$f_j(t) = \prod_{0 \leq i \leq p-1} (t - (j\tau + i)) - \prod_{0 \leq i \leq p-1} (-j\tau - i).$$

It is clear to check that $f_j(t)$ has roots $0, 1, \dots, p-1, (\text{mod } p)$. Then by the degree argument, one sees that $f_j(t) = t^p - t$, again in mod p . Thus the result follows. \square

Lemma 4.0.2. *Let G be a cyclic p -group generated by g . In the \mathbf{k} -algebra $A = \mathbf{k}\langle G, x \rangle$, suppose the relation $gx - xg = \mu(g - g^2)$ holds for some $\mu \in \mathbf{k}$. Then we have $(g)(\text{ad } x)^{p-1} = \mu^{p-1}(g - g^p)$. Moreover in the tensor algebra $A \otimes A$, we have $(x \otimes 1 + g \otimes x)^p = x^p \otimes 1 + g^p \otimes x^p + \mu^{p-1}(g - g^p) \otimes x$.*

Proof. By applying Lemma 4.0.1 (1), with $\delta(g) = (g)(\text{ad } \frac{x}{\mu})$, then we have $\delta^{p-1}(g) = \frac{1}{\mu^{p-1}}(g)(\text{ad } x)^{p-1} = g - g^p$. Hence, $(g)(\text{ad } x)^{p-1} = \mu^{p-1}(g - g^p)$. Now the statement holds by applying Proposition 2.3.1, $(x \otimes 1 + g \otimes x)^p = x^p \otimes 1 + g^p \otimes x^p + (g)(\text{ad } x)^{p-1} \otimes x$.

Alternatively, one may also derive from the argument in [20, Corollary 4.10] and [24] to show the result. \square

Before we deal with each case in Table 2, we state our strategy to determine all possible liftings from $\text{gr } H$ to H . Suppose $\text{gr } H = \mathbf{k}\langle x_1, x_2, \dots \rangle / (f_1, f_2, \dots)$ with coalgebra structure defined on x_i . By the structure of pointed coalgebras, one sees clearly that the generators x_i of $\text{gr } H$ can be lifted up to be generators of H where the coalgebra structure remains the same once $x_i \in H_1$. The case (C) is the only exception since we have one generator which is not in H_1 , whose coalgebra structure can be uniquely lifted is proved by computing the Hochschild cohomology. In the Hopf algebra H , the old relations f_i in $\text{gr } H$ becomes $f_i = r_i$ where $r_i \in H_{n-1}$ if the homogenous relation f_i has degree n in $\text{gr } H$. Second, we compute the comultiplication of each $r_i = f_i$ in H . Based on the calculation, we explicitly construct some term a_i to make $r_i - a_i$ skew-primitive, or $r_i - a_i \in H_1$. Next we can write $r_i - a_i$ as a linear combination of group like elements and skew-primitive elements of H with suitable coefficients. Finally, we need to check that all the coefficients are compatible in the way that the whole algebra modulo these relations is of dimension p^3 .

In the following subsections, for completeness, we provide as much lifting details as possible. The readers may check closely for the argument of one case and the other cases should follow similarly, possibly with additional complications arising from the structure of each case.

4.1. Liftings for Case (A). Following the above plan and applying Lemmas 4.0.1 and 4.0.2 frequently in our calculations, we will do the liftings for each case.

Case (A1). It is clear that H is the quotient of the free algebra $\mathbf{k}\langle g, x, y \rangle$, where $x, y \in H$ are liftings of $a, b \in \text{gr } H$, respectively, subject to the relations

$$g^p = 1, \quad gx - xg = r_1, \quad gy - yg = r_2, \quad x^p = r_3, \quad y^p = r_4, \quad xy - yx = r_5,$$

for some $r_1, r_2 \in H_0$, $r_5 \in H_1$ and $r_3, r_4 \in H_{p-1}$. The coalgebra structure is determined by

$$\Delta(g) = g \otimes g, \Delta(x) = x \otimes 1 + g \otimes x, \Delta(y) = y \otimes 1 + g^u \otimes y,$$

for some $0 \leq u \leq p-1$. We first determine r_1 and r_2 .

$$\begin{aligned} \Delta(r_1) &= \Delta(gx - xg) = (g \otimes g)(x \otimes 1 + g \otimes x) - (x \otimes 1 + g \otimes x)(g \otimes g) \\ &= (gx - xg) \otimes g + g^2 \otimes (gx - xg) = r_1 \otimes g + g^2 \otimes r_1. \end{aligned}$$

Since $r_1 \in H_0 = \mathbf{k}C_p$. It is easy to see that we can write $r_1 = \gamma(g - g^2)$, for some $\gamma \in \mathbf{k}$. By a suitable rescaling of the variable x , we can take $\gamma \in \{0, 1\}$. In the following, we use the notation $r_1 = \epsilon_1 g(1 - g)$, where $\epsilon_1 \in \{0, 1\}$. Similarly, we have $r_2 = \epsilon_2 g(1 - g^u)$, for $\epsilon_2 \in \{0, 1\}$.

Next, we apply 4.0.2 to get

$$\Delta(r_3) = \Delta(x^p) = (x \otimes 1 + g \otimes x)^p = x^p \otimes 1 + 1 \otimes x^p + \epsilon_1(g - 1) \otimes x$$

since $g^p = 1$, and $\epsilon_1^n = \epsilon_1$, for any $n \geq 0$ and $\epsilon_1 \in \{0, 1\}$ in this case. So

$$\begin{aligned} \Delta(r_3 - \epsilon_1 x) &= x^p \otimes 1 + 1 \otimes x^p + \epsilon_1(g \otimes x - 1 \otimes x) - \epsilon_1(x \otimes 1 + g \otimes x) \\ &= (x^p - \epsilon_1 x) \otimes 1 + 1 \otimes (x^p - \epsilon_1 x). \end{aligned}$$

Hence, $(r_3 - \epsilon_1 x)$ is primitive. For r_4 , we use the fact that $[-, y]$ is a derivation, so $[g^u, y] = u g^{u-1} [g, y] = u \epsilon_2 g^u (1 - g^u)$. Hence, by applying 4.0.2 again, we obtain $(r_4 - u^{p-1} \epsilon_2 y)$ is primitive.

Moreover, we get

$$\begin{aligned} \Delta(r_5) &= \Delta(xy - yx) \\ &= (x \otimes 1 + g \otimes x)(y \otimes 1 + g^u \otimes y) - (y \otimes 1 + g^u \otimes y)(x \otimes 1 + g \otimes x) \\ &= (xy - yx) \otimes 1 + g^{u+1} \otimes (xy - yx) + (xg^u - g^u x) \otimes y + (gy - yg) \otimes x \\ &= r_5 \otimes 1 + g^{u+1} \otimes r_5 - u \epsilon_1 (g^u - g^{u+1}) \otimes y + \epsilon_2 (g - g^{u+1}) \otimes x. \end{aligned}$$

Then it is easy to see that

$$\Delta(r_5 + u \epsilon_1 y - \epsilon_2 x) = (r_5 + u \epsilon_1 y - \epsilon_2 x) \otimes 1 + g^{u+1} \otimes (r_5 + u \epsilon_1 y - \epsilon_2 x).$$

Finally, we point out that if $u \neq 0$, then the primitive space $P(H) = 0$. Otherwise, if $u = 0$, then $P(H) = \mathbf{k}y$ and $\Delta(r_5) = r_5 \otimes 1 + g \otimes r_5$. Therefore, we obtain the following two cases depending on the value of u .

- **(A1a)** Suppose $u = 0$. Then H is the quotient of the free algebra $\mathbf{k}\langle g, x, y \rangle$ modulo the possible relations

$$\begin{aligned} g^p &= 1, \quad gx - xg = \epsilon_1 (g - g^2), \quad gy = yg, \quad x^p = \epsilon_1 x + \lambda y, \\ y^p &= \mu y, \quad xy - yx = \sigma x + \tau (1 - g), \end{aligned}$$

for some $\epsilon_1 \in \{0, 1\}$ and some $\lambda, \mu, \sigma, \tau \in \mathbf{k}$. By rescaling of y , we can let $\mu = \epsilon_2 \in \{0, 1\}$. Since H is of dimension p^3 , the Diamond Lemma [7] implies

that all the ambiguities of the relations are resolvable. This can be done by comparing coefficients of each of the following expressions:

$$[x, x^p], [y, x^p], [g, x^p], [x, y^p], [y, y^p], [g, y^p], [x, g^p], [y, g^p],$$

where each expression is computed in two ways: (i) by replacing the above x^p, y^p, g^p relations in the commutator, and (ii) by using Proposition 2.3.1, e.g. $[y, x^p] = (y)(\text{ad } x)^p$. Then we get the compatible conditions for the coefficients:

$$\epsilon_1 \sigma = \lambda \sigma = \lambda \tau = (\epsilon_2 - \sigma^{p-1}) \sigma = (\epsilon_2 - \sigma^{p-1}) \tau = 0.$$

We may interpret these conditions further:

- Suppose $\epsilon_1 = \epsilon_2 = 0$. Then we have $\sigma = 0$ and $\lambda \tau = 0$. By rescaling x, y , we can take $\lambda, \tau \in \{0, 1\}$ satisfying $\lambda \tau = 0$. There are totally three classes.
 - Suppose $\epsilon_1 = 0, \epsilon_2 = 1$. Then we have $\lambda \sigma = \lambda \tau = 0$ and $\sigma^p = \sigma, \tau = \sigma^{p-1} \tau$. By rescaling x, y , we can take $\sigma, \lambda, \tau \in \{0, 1\}$ satisfying $\lambda \sigma = \tau(1 - \sigma) = 0$. There are totally four classes.
 - Suppose $\epsilon_1 = 1, \epsilon_2 = 0$. Then we have $\sigma = \lambda \tau = 0$. By rescaling x, y , we can take $\lambda, \tau \in \{0, 1\}$ satisfying $\lambda \tau = 0$. There are totally three classes.
 - Suppose $\epsilon_1 = \epsilon_2 = 1$. Then we have $\sigma = \tau = 0$. We get one infinite family of H whose structures depending on $\lambda \in \mathbf{k}$.
- **(A1b)** Suppose $u \neq 0$. Then H is the quotient of the free algebra $\mathbf{k}\langle g, x, y \rangle$ modulo the possible relations

$$\begin{aligned} g^p &= 1, \quad gx - xg = \epsilon_1 (g - g^2), \quad gy - yg = \epsilon_2 (g - g^{u+1}), \quad x^p = \epsilon_1 x, \\ y^p &= \epsilon_2 y, \quad xy - yx + u\epsilon_1 y - \epsilon_2 x = \tau (1 - g^{u+1}), \end{aligned}$$

for some $\epsilon_i \in \{0, 1\}$ and some $\tau \in \mathbf{k}$.

When we apply the Diamond Lemma [7], all the ambiguities of the relations are resolvable and there is no ambiguity condition in this case. Here we will check for $[g, y^p]$, $[x, y^p]$ and $[y, x^p]$ and leave the rest to the readers. For $[g, y^p]$, take $\delta = \text{ad } y$ and $\delta(g) = \epsilon_2 (g - g^{u+1})$. One checks that either (i) $[g, y^p] = [g, \epsilon_2 y] = \epsilon_2 [g, y]$, or (ii) $[g, y^p] = (g)(\text{ad } y)^p = \delta^p(g) = \delta(g) = [g, y]$ by Lemma 4.0.1 (3). Then both ways are the same since $\epsilon_2 \in \{0, 1\}$. For $[x, y^p]$ and $[y, x^p]$, we need the following result.

Claim: $\sum_{i=0}^{p-2} (u\epsilon_1)^i (g^{u+1})(\text{ad } x)^{p-1-i} = \sum_{i=0}^{p-2} \epsilon_2^i (g^{u+1})(\text{ad } y)^{p-1-i} = 0$.

Proof of claim. Without loss of generality, we assume $\epsilon_1 = \epsilon_2 = 1$. For the first summation, take $\delta = \text{ad } x$ and $\delta(g) = g - g^2$. Thus, by Fermat's Little Theorem, for $u \neq 0$, $u^{p-1} = 1$ in mod p , and we have:

$$\sum_{i=0}^{p-2} (u\epsilon_1)^i (g^{u+1})(\text{ad } x)^{p-1-i} = \left(\sum_{i=0}^{p-2} \frac{u^i}{u^{p-1}} \delta^{p-1-i} \right) (g^{u+1})$$

$$\begin{aligned}
&= \left(\sum_{i=0}^{p-2} \delta^{p-1-i} / u^{p-1-i} \right) (g^{u+1}) \\
&= (\delta/u + \delta^2/u^2 + \cdots + \delta^{p-1}/u^{p-1})(g^{u+1}) = 0
\end{aligned}$$

by 4.0.1 (2). For the second summation, take $\delta = (\text{ad } y)/u$ and $\delta(g^u) = g^{u-1}(g - g^{u+1}) = g^u(1 - g^u)$. For simplicity, we change the generator of the cyclic group $G = C_p$ from g to $h = g^u$. So $\delta(h) = h - h^2$. Thus

$$\begin{aligned}
\sum_{i=0}^{p-2} (g^{u+1})(\text{ad } y)^{p-1-i} &= \left(\sum_{i=0}^{p-2} (\delta u)^{p-1-i} \right) (h^{1+u^{-1}}) \\
&= (\delta u + \delta^2 u^2 + \cdots + \delta^{p-1} u^{p-1})(h^{1+u^{-1}}) = 0.
\end{aligned}$$

by 4.0.1 (2) again. □

Moreover, by induction on n , one can prove that for all $n \geq 1$:

$$\begin{aligned}
(y)(\text{ad } x)^n &= (u\epsilon_1)^{n-1}[y, x] + \tau \left(\sum_{i=0}^{n-2} (u\epsilon_1)^i (g^{u+1})(\text{ad } x)^{n-1-i} \right), \text{ and} \\
(x)(\text{ad } y)^n &= \epsilon_2^{n-1}[x, y] - \tau \left(\sum_{i=0}^{n-2} \epsilon_2^i (g^{u+1})(\text{ad } y)^{n-1-i} \right).
\end{aligned}$$

Hence, one gets either (i) $[x, y^p] = [x, \epsilon_2 y] = \epsilon_2[x, y]$, or (ii) $[x, y^p] = x(\text{ad } y)^p = \epsilon_2^{p-1}[x, y] - \tau(\sum_{i=0}^{p-2} \epsilon_2^i (g^{u+1})(\text{ad } y)^{p-1-i}) = \epsilon_2^{p-1}[x, y]$ by the claim. So both ways are the same. The expression $[y, x^p]$ can be checked similarly.

In conclusion, if one of the ϵ_i 's is zero, we can always rescale x or y to make $\tau \in \{0, 1\}$, where, depending on $u \in \{1, 2, \dots, p-1\}$, there are totally $6(p-1)$ classes. When $\epsilon_1 = \epsilon_2 = 1$, we get $(p-1)$ infinite families of H whose structures depending on $\tau \in \mathbf{k}$ and $u \in \{1, 2, \dots, p-1\}$.

Case (A2). It is clear that H is the quotient of the free algebra $\mathbf{k}\langle g, x, y \rangle$, where $x, y \in H$ are liftings of $a, b \in \text{gr } H$, respectively, subject to the relations

$$g^p = 1, \quad gx - xg = r_1, \quad gy - yg = r_2, \quad x^p = r_3, \quad y^p = r_4, \quad xy - yx = r_5,$$

for some $r_1, r_2 \in H_0$, $r_5 \in H_1$ and $r_3, r_4 \in H_{p-1}$. The coalgebra structure is determined by

$$\Delta(g) = g \otimes g, \quad \Delta(x) = x \otimes 1 + 1 \otimes x, \quad \Delta(y) = y \otimes 1 + 1 \otimes y.$$

Here, the primitive space is given by $P(H) = \mathbf{k}x \oplus \mathbf{k}y$. Similar computations as before, we have:

$$\begin{aligned}
\Delta(r_1) &= r_1 \otimes g + g \otimes r_1; \text{ and} \\
\Delta(r_2) &= r_2 \otimes g + g \otimes r_2.
\end{aligned}$$

Since $r_1, r_2 \in H_0 = \mathbf{k}C_p$, we have $r_1 = \gamma_1(g - g) = 0$ and $r_2 = \gamma_2(g - g) = 0$, for some $\gamma_1, \gamma_2 \in \mathbf{k}$. Moreover,

$$\begin{aligned}\Delta(r_3) &= \Delta(x^p) = (x \otimes 1 + 1 \otimes x)^p = r_3 \otimes 1 + 1 \otimes r_3 \\ \Delta(r_4) &= \Delta(y^p) = (y \otimes 1 + 1 \otimes y)^p = r_4 \otimes 1 + 1 \otimes r_4 \\ \Delta(r_5) &= \Delta(xy - yx) = r_5 \otimes 1 + 1 \otimes r_5.\end{aligned}$$

Thus, r_3, r_4 , and r_5 are primitive elements and the possible relations in H are:

$$g^p = 1, \quad gx = xg, \quad gy = yg, \quad x^p = \lambda x + \mu y, \quad y^p = \sigma x + \tau y, \quad xy - yx = \alpha x + \beta y,$$

for some $\lambda, \mu, \sigma, \tau, \alpha, \beta \in \mathbf{k}$. Again, by Diamond Lemma [7], all the ambiguities of the relations are resolvable. In this case, the primitive space $P(H) = \mathbf{k}x \oplus \mathbf{k}y$ is indeed a two-dimensional restricted Lie algebra. We can apply the classifications in [25, Theorem 7.4 (1)-(5)] and obtain the following five classes of H :

- **(A2-a):** $\mathbf{k}\langle x, y, g \rangle / (g^p = 1, x^p = 0, y^p = 0, [g, x] = [g, y] = 0, [x, y] = 0)$
- **(A2-b):** $\mathbf{k}\langle x, y, g \rangle / (g^p = 1, x^p = x, y^p = 0, [g, x] = [g, y] = 0, [x, y] = 0)$
- **(A2-c):** $\mathbf{k}\langle x, y, g \rangle / (g^p = 1, x^p = y, y^p = 0, [g, x] = [g, y] = 0, [x, y] = 0)$
- **(A2-d):** $\mathbf{k}\langle x, y, g \rangle / (g^p = 1, x^p = x, y^p = y, [g, x] = [g, y] = 0, [x, y] = 0)$
- **(A2-e):** $\mathbf{k}\langle x, y, g \rangle / (g^p = 1, x^p = x, y^p = 0, [g, x] = [g, y] = 0, [x, y] = y),$

with coalgebra structures $\Delta(g) = g \otimes g$, $\Delta(x) = x \otimes 1 + 1 \otimes x$, $\Delta(y) = y \otimes 1 + 1 \otimes y$ occur in all five classes.

Case (A3), $p = 2$. It is clear that H is the quotient of the free algebra $\mathbf{k}\langle g, x, y \rangle$, where $x, y \in H$ are liftings of $a, b \in \text{gr } H$, respectively, subject to the relations

$$g^p = 1, \quad gx - xg = r_1, \quad gy - yg = r_2, \quad x^p = r_3, \quad y^p = r_4, \quad xy - yx = r_5,$$

for some $r_1, r_2 \in H_0$, $r_5 \in H_1$ and $r_3, r_4 \in H_{p-1}$. The coalgebra structure is determined by

$$\Delta(g) = g \otimes g, \quad \Delta(x) = x \otimes 1 + 1 \otimes x, \quad \Delta(y) = y \otimes 1 + 1 \otimes y.$$

The computation is very similar to case (A2) and yields the same ambiguity relations. By applying [25, Theorem 7.4 (1)-(5)] again, we also get five classes of H :

- **(A3-a):** $\mathbf{k}\langle x, y, g \rangle / (g^p = 1, x^p = 0, y^p = 0, gx = yg, gy = xg, [x, y] = 0)$
- **(A3-b):** $\mathbf{k}\langle x, y, g \rangle / (g^p = 1, x^p = x, y^p = 0, gx = yg, gy = xg, [x, y] = 0)$
- **(A3-c):** $\mathbf{k}\langle x, y, g \rangle / (g^p = 1, x^p = y, y^p = 0, gx = yg, gy = xg, [x, y] = 0)$
- **(A3-d):** $\mathbf{k}\langle x, y, g \rangle / (g^p = 1, x^p = x, y^p = y, gx = yg, gy = xg, [x, y] = 0)$
- **(A3-e):** $\mathbf{k}\langle x, y, g \rangle / (g^p = 1, x^p = x, y^p = 0, gx = yg, gy = xg, [x, y] = y),$

with coalgebra structures $\Delta(g) = g \otimes g$, $\Delta(x) = x \otimes 1 + 1 \otimes x$, $\Delta(y) = y \otimes 1 + 1 \otimes y$ occur in all five classes.

4.2. Liftings for Case (B), $p > 2$. It is clear that H is the quotient of the free algebra $\mathbf{k}\langle g, x, y \rangle$, where $x, y \in H$ are liftings of $a, b \in \text{gr } H$, respectively, subject to the relations

$$g^p = 1, \quad gx - xg = r_1, \quad gy - (x + y)g = r_2, \quad x^p = r_3, \quad y^p = r_4, \quad xy - yx - \frac{1}{2}x^2 = r_5,$$

for some $r_1, r_2 \in H_0$, $r_5 \in H_1$ and $r_3, r_4 \in H_{p-1}$. The coalgebra structure is determined by

$$\Delta(g) = g \otimes g, \quad \Delta(x) = x \otimes 1 + g \otimes x, \quad \Delta(y) = y \otimes 1 + g \otimes y.$$

Here, $P(H) = 0$. One computes:

$$\Delta(r_1) = r_1 \otimes g + g^2 \otimes r_1; \text{ and}$$

$$\Delta(r_2) = r_2 \otimes g + g^2 \otimes r_2.$$

Since $r_1, r_2 \in H_0 = \mathbf{k}C_p$, by rescaling the variables, we may write $r_1 = \epsilon_1(g - g^2)$ and $r_2 = \mu(g - g^2)$, for $\epsilon_1 \in \{0, 1\}$ and $\mu \in \mathbf{k}$.

Next, by applying 4.0.2 and similar argument as in case (A1), we have

$$\Delta(r_3 - \epsilon_1 x) = (x^p - \epsilon_1 x) \otimes 1 + 1 \otimes (x^p - \epsilon_1 x).$$

Hence, $(r_3 - \epsilon_1 x)$ is primitive. This implies $r_3 = \epsilon_1 x$ since $P(H) = 0$.

$$\begin{aligned} \Delta(r_5) &= \Delta(xy - yx - \frac{1}{2}x^2) \\ &= r_5 \otimes 1 + g^2 \otimes r_5 + (xg - gx) \otimes y + (gy - yg - \frac{1}{2}xg - \frac{1}{2}gx) \otimes x \\ &= r_5 \otimes 1 + g^2 \otimes r_5 - \epsilon_1(g - g^2) \otimes y + \mu(g - g^2) \otimes x - \frac{1}{2}\epsilon_1(g - g^2) \otimes x. \end{aligned}$$

One can check that

$$\Delta(r_5 + \epsilon_1 y - \mu x + \frac{1}{2}\epsilon_1 x) = (r_5 + \epsilon_1 y - \mu x + \frac{1}{2}\epsilon_1 x) \otimes 1 + g^2 \otimes (r_5 + \epsilon_1 y - \mu x + \frac{1}{2}\epsilon_1 x)$$

So $(r_5 + \epsilon_1 y - \mu x + \frac{1}{2}\epsilon_1 x)$ is $(1, g^2)$ -skew primitive. One can write $r_5 + \epsilon_1 y - \mu x + \frac{1}{2}\epsilon_1 x = \tau(1 - g^2)$, for some $\tau \in \mathbf{k}$. In other words, $xy - yx = \frac{1}{2}x^2 - \epsilon_1 y + (\mu - \frac{1}{2}\epsilon_1)x + \tau(1 - g^2)$.

Case (B) becomes very complicated when it comes to computing the relation $r_4 = y^p$, due to how $(g)(\text{ad } y) = [g, y] = gy - yg$ involves both x and g terms as we have seen in r_2 computation above. Therefore, we specify it to the smallest case when $p = 3$ and leave the general p case for future task:

Case (B) for $p = 3$: We have the following relations

$$g^3 = 1, \quad gx - xg = r_1, \quad gy - (x + y)g = r_2, \quad x^3 = r_3, \quad y^3 = r_4, \quad xy - yx - \frac{1}{2}x^2 = r_5,$$

with the coalgebra structure

$$\Delta(g) = g \otimes g, \quad \Delta(x) = x \otimes 1 + g \otimes x, \quad \Delta(y) = y \otimes 1 + g \otimes y.$$

As before, we can write $r_1 = \epsilon(g - g^2)$, $r_2 = \mu(g - g^2)$, $r_3 = \epsilon x$ and $r_5 = (\mu - \frac{1}{2}\epsilon)x - \epsilon y + \tau(1 - g^2)$, for some $\epsilon \in \{0, 1\}$ and $\mu, \tau \in \mathbf{k}$. For r_4 , using the relations

$$gy = yg + xg + \mu(g - g^2), \quad gx = xg + \epsilon(g - g^2), \quad xy = yx + \frac{1}{2}x^2 + (\mu - \frac{1}{2}\epsilon)x - \epsilon y + \tau(1 - g^2),$$

we compute in mod 3

$$\Delta(y^2) = y^2 \otimes 1 + (2yg + xy + \mu g - \mu g^2) \otimes y + g^2 \otimes y^2,$$

and

$$\begin{aligned} \Delta(y^3) &= (y \otimes 1 + g \otimes y) (y^2 \otimes 1 + (2yg + xg + \mu(g - g^2)) \otimes y + g^2 \otimes y^2) \\ &= y^3 \otimes 1 + (2y^2g + yxg + \mu y(g - g^2) + gy^2) \otimes y \\ &\quad + (yg^2 + 2gyg + gxg + \mu(g^2 - 1)) \otimes y^2 + g^3 \otimes y^3 \\ &= y^3 \otimes 1 + (\epsilon xg - \epsilon yg - \mu \epsilon g^2 + (\tau + \mu^2)g + (\mu \epsilon - \tau - \mu^2)) \otimes y \\ &\quad + \epsilon(g^2 - 1) \otimes y^2 + 1 \otimes y^3. \end{aligned}$$

Therefore,

$$\begin{aligned} \Delta(y^3 - \epsilon y^2 + (\mu \epsilon - \tau - \mu^2)y) &= (y^3 - \epsilon y^2 + (\mu \epsilon - \tau - \mu^2)y) \otimes 1 \\ &\quad + 1 \otimes (y^3 - \epsilon y^2 + (\mu \epsilon - \tau - \mu^2)y). \end{aligned}$$

So we have $(y^3 - \epsilon y^2 + (\mu \epsilon - \tau - \mu^2)y)$ is primitive, which is 0, so $y^3 = r_4 = \epsilon y^2 - (\mu \epsilon - \tau - \mu^2)y$. The relations in H (when $p = 3$) are

$$\begin{aligned} g^3 &= 1, \quad gx - xg = \epsilon(g - g^2), \quad gy - yg = xg + \mu(g - g^2), \quad x^3 = \epsilon x, \\ y^3 &= \epsilon y^2 - (\mu \epsilon - \tau - \mu^2)y, \quad xy - yx = -x^2 + (\epsilon + \mu)x - \epsilon y + \tau(1 - g^2) \end{aligned}$$

for some $\epsilon \in \{0, 1\}$ and $\mu, \tau \in \mathbf{k}$. When we apply the Diamond Lemma [7], all the ambiguities of the relations are resolvable and there is no ambiguity condition in this case. For instance, we have

$$\begin{aligned} [g, x] &= \epsilon(g - g^2) \\ [g, x^2] &= -\epsilon xg + \epsilon xg^2 + \epsilon(g - 1) \\ [g^2, x] &= \epsilon(1 - g^2) \\ [g, y] &= xg + \mu(g - g^2) \\ [g^2, y] &= -xg^2 + (\epsilon - \mu)(g^2 - 1) \\ [g, y^2] &= -yxg + \epsilon xg - (\mu + \epsilon)yg + \mu yg^2 + (\mu \epsilon - \mu^2 - \tau) + (\tau + \mu^2)g - \mu \epsilon g^2 \\ [x^2, y] &= -(\tau + \mu \epsilon)x - \mu x^2 + \tau xg^2 + \epsilon yx + \epsilon y + \epsilon \tau(1 - g^2) \\ [x, y^2] &= yx^2 + (\epsilon - \mu)yx + \epsilon y^2 + (\epsilon - \tau - \epsilon \mu)y + (\tau + \epsilon + \mu^2)x - \epsilon x^2 + \tau yg^2 + \tau \epsilon - \tau \epsilon g^2. \end{aligned}$$

Hence,

$$\begin{aligned} [g, y^3] &= [g, \epsilon y^2 - (\mu \epsilon - \tau - \mu^2)y] \\ &= -\epsilon yxg + (\tau + \mu^2 - \mu \epsilon + \epsilon)xg - (\epsilon \mu + \epsilon)yg + \mu \epsilon yg^2 + (\mu \epsilon - \epsilon \tau - \mu^2 \epsilon) \\ &\quad + (\epsilon \tau + \tau \mu + \mu^3)g + (\mu^2 \epsilon - \mu \epsilon - \tau \mu - \mu^3)g^2 \end{aligned}$$

$$= [[[g, y], y], y],$$

and

$$\begin{aligned} [x, y^3] &= [g, \epsilon y^2 - (\mu\epsilon - \tau - \mu^2)y] \\ &= \epsilon y x^2 + (\epsilon - \epsilon\mu)yx + \epsilon y^2 + (\epsilon + \tau\epsilon - \mu^2\epsilon)y + (\epsilon\mu^2 + \tau\mu + \epsilon + \mu^3 - \tau\epsilon - \epsilon\mu)x \\ &\quad + (\mu\epsilon - \tau - \mu^2 - \epsilon)x^2 + \tau\epsilon y g^2 + (\tau\epsilon + \tau^2 + \tau\mu^2 - \tau\mu\epsilon)(1 - g^2) \\ &= [[[x, y], y], y]. \end{aligned}$$

We may interpret these conditions further:

- When $\epsilon = \mu = 0$, by rescaling of both x and y , we can further let $\tau \in \{0, 1\}$. There are two classes of H .
- When $\epsilon = 0$ and $\mu \neq 0$, by rescaling of x and y by the same factor, we can further let $\mu = 1$. There is one infinite family of H depending on $\tau \in \mathbf{k}$.
- When $\epsilon = 1$, there is one infinite family of H depending on two parameters $\mu, \tau \in \mathbf{k}$.

In positive characteristic $p > 3$, we conjecture that the lifting of case (B) is

$$\begin{aligned} g^p &= 1, \quad gx - xg = \epsilon(g - g^2), \quad gy - yg = xg + \mu(g - g^2), \quad x^p = \epsilon x, \\ y^p &= f_{p-1}y^{p-1} + \cdots + f_1y, \quad xy - yx = \frac{1}{2}x^2 + (\mu - \frac{1}{2}\epsilon)x - \epsilon y + \tau(1 - g^2), \end{aligned}$$

where $\epsilon \in \{0, 1\}$ and $\mu, \tau \in \mathbf{k}$ and f_i 's are polynomials in terms of ϵ, μ, τ . Moreover, the isomorphism classes are given similarly as in the case $p = 3$ above.

4.3. Liftings for Case (C). It is clear that H is the quotient of the free algebra $\mathbf{k}\langle g, x, y \rangle$, where $x, y \in H$ are liftings of $a, b \in \text{gr } H$, respectively, subject to the relations

$$g^p = 1, \quad gx - xg = r_1, \quad gy - yg = r_2, \quad x^p = r_3, \quad y^p = r_4, \quad xy - yx = r_5,$$

for some $r_1 \in H_0$, $r_2, r_3 \in H_{p-1}$, $r_5 \in H_p$ and $r_4 \in H_{p^2-1}$. The coalgebra structure is determined by

$$\Delta(g) = g \otimes g, \quad \Delta(x) = x \otimes 1 + g^\epsilon \otimes x, \quad \Delta(y) = y \otimes 1 + 1 \otimes y + \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{\epsilon(p-i)} \otimes x^{p-i},$$

where $g^\epsilon = 1$ or g . In order to show that the lifting of the comultiplication of y is unique, we need the following result.

Claim: Let A be the Hopf subalgebra of H generated by $\{g, x\}$ with relations

$$A = \mathbf{k}\langle g, x \rangle / (g^p - 1, x^p - \epsilon x, gx - xg - \epsilon(g - g^2)),$$

for $\epsilon \in \{0, 1\}$. Then $\dim H^2(\Omega A) = 1$ and it is spanned by the 2-cocycle

$$\sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{\epsilon(p-i)} \otimes x^{p-i}.$$

Proof of claim. Suppose $\epsilon = 1$. By the classification result of pointed Hopf algebras of dimension p^2 over \mathbf{k} [24], A is the only class that is both non-commutative and non-cocommutative. Hence it must be self dual and $A^* \cong A$ as Hopf algebras.

Suppose $\epsilon = 0$. Then A is local and $\dim J/J^2 = 2$, where J is the augmentation ideal of A . So $A^* \cong u(\mathfrak{g})$ for some two-dimensional restricted Lie algebra \mathfrak{g} . Note that A is non-cocommutative. So \mathfrak{g} is non-abelian. By [25, Theorem 7.4], $\mathfrak{g} = \mathbf{k}x + \mathbf{k}y$ satisfying $x^p = x$, $y^p = 0$ and $[x, y] = y$.

Then it is clear to see that, as algebras, $A^* \cong \mathbf{k}C_p \# K$, where $K = \mathbf{k}[x]/(x^p - x)$ with $\Delta(x) = x \otimes 1 + 1 \otimes x$ and C_p is the cyclic group of order p generated by g . The K -action on $\mathbf{k}C_p$ is given by $x \cdot g = g^2 - g$ if $\epsilon = 1$, or $x \cdot g = g + 1$ if $\epsilon = 0$. Now we can apply the spectral sequence used in Proposition 1.5.5 to conclude that

$$\dim H^2(\Omega A) = \dim \mathrm{HH}^2(A^*, \mathbf{k}) = \dim \mathrm{HH}^2(\mathbf{k}C_p, \mathbf{k})^K \leq \dim \mathrm{HH}^2(\mathbf{k}C_p) = 1.$$

Next one checks that the element $\sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{\epsilon(p-i)} \otimes x^{p-i}$ is a 2-cocycle in ΩA and does not lie in the coboundary. Hence, $\dim H^2(\Omega A) \geq 1$. So it must equal one. This proves the claim. \square

We obtain two cases depending on the value of ϵ :

- **(Ca)** Suppose $\epsilon = 0$. Then $P(H) = \mathbf{k}x$, $\Delta(y) = y \otimes 1 + 1 \otimes y + \omega(x)$, for the notation $\omega(x)$ as in Equation (3.2.0.1), and

$$\Delta(r_1) = \Delta(gx - xg) = r_1 \otimes g + g \otimes r_1.$$

Since $r_1 \in H_0$, we can write $r_1 = \gamma_1(g - g) = 0$, for some $\gamma_1 \in \mathbf{k}$, that is, $gx = xg$. And

$$\Delta(r_3) = \Delta(x^p) = r_3 \otimes 1 + 1 \otimes r_3.$$

So r_3 is primitive. By rescaling both x and y , we may write $r_3 = \epsilon_3 x$, for some $\epsilon_3 \in \{0, 1\}$.

$$\begin{aligned} \Delta(r_2) &= \Delta(gy - yg) = gy \otimes g + g \otimes gy + \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} gx^i \otimes gx^{p-i} \\ &\quad - yg \otimes g - g \otimes yg - \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g \otimes x^{p-i} g \\ &= r_2 \otimes g + g \otimes r_2, \end{aligned}$$

since $gx^i = x^i g$, for any $i \geq 0$. Thus, we can write $r_2 = \gamma_2(g - g) = 0$, for some $\gamma_2 \in \mathbf{k}$, that is, $gy = yg$. Similarly, one checks

$$\Delta(r_5) = \Delta(xy - yx) = 1 \otimes (xy - yx) + (xy - yx) \otimes 1.$$

So r_5 is primitive, we can write $r_5 = \sigma x$, for some $\sigma \in \mathbf{k}$.

For r_4 , with all the relations we have in H , one sees that

$$\omega(x) (\mathrm{ad} (\lambda \omega(x) + y \otimes 1 + 1 \otimes y))^{p-1} = \omega(x) (\mathrm{ad} (y \otimes 1 + 1 \otimes y))^{p-1}$$

in $H \otimes H$. Then by Proposition 2.3.1,

$$\Delta(r_4) = \Delta(y^p) = y^p \otimes 1 + 1 \otimes y^p + \omega(x)^p + \omega(x) (\mathrm{ad} (y \otimes 1 + 1 \otimes y))^{p-1}$$

$$= y^p \otimes 1 + 1 \otimes y^p + \omega(x^p) + \rho_y^{p-1}(\omega(x)),$$

where we use notations in [16] to write $\rho_y(\omega(x)) = [\omega(x), y \otimes 1 + 1 \otimes y]$ and $\rho_y(x) = [x, y]$. We get two smaller cases depending on the characteristic of \mathbf{k} :

– (Ca') Suppose $\text{char.}\mathbf{k} = 2$. Then

$$\begin{aligned} \rho_y(\omega(x)) &= [\omega(x), y \otimes 1 + 1 \otimes y] = [x \otimes x, y \otimes 1 + 1 \otimes y] \\ &= [x, y] \otimes x + x \otimes [x, y] = 2\sigma x \otimes x = 0. \end{aligned}$$

Thus, one has:

$$\Delta(r_4) = y^p \otimes 1 + 1 \otimes y^p + \omega(x^p) + \rho_y^{p-1}(\omega(x)) = r_4 \otimes 1 + 1 \otimes r_4 + \epsilon_3 \omega(x).$$

It is easy to check that $(r_4 - \epsilon_3 y)$ is primitive, so $r_4 - \epsilon_3 y = \tau x$, for some $\tau \in \mathbf{k}$, since $P(H) = \mathbf{k}x$. We have $r_4 = y^p = \tau x + \epsilon_3 y$.

For case (Ca') when $p = 2$, the possible relations in H are:

$$g^p = 1, \quad gx = xg, \quad gy = yg, \quad x^p = \epsilon_3 x, \quad y^p = \tau x + \epsilon_3 y, \quad xy - yx = \sigma x,$$

for some $\sigma, \tau \in \mathbf{k}$ and $\epsilon_3 \in \{0, 1\}$. By Diamond Lemma [7], we get the following compatible conditions for the coefficients:

$$\epsilon_3 \sigma = (\epsilon_3 - \sigma^{p-1})\sigma = \tau \sigma = 0.$$

Here if $\epsilon_3 \sigma = 0$, then we will have $\sigma^p = 0$ which implies that $\sigma = 0$ and it is easy to see then $\sigma = 0$ is the only restriction.

– (Ca'') Suppose $\text{char.}\mathbf{k} \neq 2$. Thus, by applying formula in [16, Proposition 2.7(iii)] where $i = p - 2$, we have:

$$\rho_y^{p-1}(\omega(x)) = \partial^1(Z) = \Delta(Z) - Z \otimes 1 - 1 \otimes Z,$$

where

$$Z := - \sum_{i_1 + \dots + i_p = p-2} \frac{(p-2)!}{i_1! \dots i_p!} \rho_y^{i_1}(x) \dots \rho_y^{i_{p-1}}(x) \rho_y^{1+i_p}(x).$$

By previous assumption, $\rho_y(x) = [x, y] = \sigma x$, for some $\sigma \in \mathbf{k}$. So for any $s \geq 0$, $\rho_y^s(x) = \sigma^s x$. When $p > 2$, Z becomes:

$$\begin{aligned} Z &= - \sum_{i_1 + \dots + i_p = p-2} \frac{(p-2)!}{i_1! \dots i_p!} \sigma^{i_1 + \dots + i_p + 1} x^p \\ &= - \sum_{i_1 + \dots + i_p = p-2} \frac{(p-2)!}{i_1! \dots i_p!} \sigma^{p-1} x^p \\ &= - \sum_{i_1 + \dots + i_p = p-2} \frac{(p-2)!}{i_1! \dots i_p!} \sigma^{p-1} \epsilon_3 x \end{aligned}$$

$$\begin{aligned}
&= -\sigma^{p-1}\epsilon_3 x \left(\sum_{i_1+\dots+i_p=p-2} \frac{(p-2)!}{i_1! \cdots i_p!} \right) \\
&= -\sigma^{p-1}\epsilon_3 x (p-2)^{p-2} = -\sigma^{p-1}\epsilon_3 x (-2^{p-2}) \\
&= \sigma^{p-1}\epsilon_3 x \frac{1}{2} 2^{p-1} = \frac{1}{2}\sigma^{p-1}\epsilon_3 x,
\end{aligned}$$

where $2^{p-1} = 1$ by Fermat's Little Theorem. It follows that $\rho_y^{p-1}(\omega(x)) = \partial^1(Z) = \Delta(Z) - Z \otimes 1 - 1 \otimes Z$. So

$$\Delta(r_4) = y^p \otimes 1 + 1 \otimes y^p + \epsilon_3 \omega(x) + \Delta(Z) - Z \otimes 1 - 1 \otimes Z.$$

Therefore,

$$\begin{aligned}
\Delta(y^p - Z) &= \Delta(r_4 - \frac{1}{2}\sigma^{p-1}\epsilon_3 x) \\
&= (r_4 - \frac{1}{2}\sigma^{p-1}\epsilon_3 x) \otimes 1 + 1 \otimes (r_4 - \frac{1}{2}\sigma^{p-1}\epsilon_3 x) + \epsilon_3 \omega(x).
\end{aligned}$$

It is easy to check that $(r_4 - \frac{1}{2}\sigma^{p-1}\epsilon_3 x - \epsilon_3 y)$ is primitive, so $r_4 - \frac{1}{2}\sigma^{p-1}\epsilon_3 x - \epsilon_3 y = \tau x$, for some $\tau \in \mathbf{k}$, or $y^p = (\tau + \frac{1}{2}\sigma^{p-1}\epsilon_3)x + \epsilon_3 y$.

For case (Ca'') where $p > 2$, the possible relations in H are:

$$\begin{aligned}
g^p &= 1, \quad gx = xg, \quad gy = yg, \\
x^p &= \epsilon_3 x, \quad y^p = (\tau + \frac{1}{2}\sigma^{p-1}\epsilon_3)x + \epsilon_3 y, \quad xy - yx = \sigma x,
\end{aligned}$$

for some $\sigma, \tau \in \mathbf{k}$ and $\epsilon_3 \in \{0, 1\}$. By Diamond Lemma [7], we get the following compatible conditions for the coefficients:

$$\epsilon_3 \sigma = (\epsilon_3 - \sigma^{p-1})\sigma = (\tau + \frac{1}{2}\sigma^{p-1}\epsilon_3)\sigma = 0.$$

Here if $\epsilon_3 \sigma = 0$, then we will have $\sigma^p = 0$ which implies that $\sigma = 0$ and it is easy to see then $\sigma = 0$ is the only restriction.

Finally, the two cases (Ca') and (Ca'') can be combined together. For case (Ca), the possible relations in H are:

$$g^p = 1, \quad gx = xg, \quad gy = yg, \quad x^p = \epsilon_3 x, \quad y^p = \tau x + \epsilon_3 y, \quad xy - yx = 0,$$

for some $\tau \in \mathbf{k}$ and $\epsilon_3 \in \{0, 1\}$.

- Suppose $\epsilon_3 = 0$. By rescaling x, y , we can further choose $\tau \in \{0, 1\}$. We get two finite classes of H .
- Suppose $\epsilon_3 = 1$. We get one infinite family of H whose structures depending on $\tau \in \mathbf{k}$.

- **(Cb)** Suppose $\epsilon = 1$. Then $P(H) = 0$ and

$$\Delta(r_1) = r_1 \otimes g + g^2 \otimes r_1.$$

Since $r_1 \in H_0$, we can write $r_1 = \epsilon_1(g - g^2)$, for $\epsilon_1 \in \{0, 1\}$. Again, by applying 4.0.2 and similar argument as in case (A1), we have $(r_3 - \epsilon_1 x)$ is primitive. This implies $r_3 = \epsilon_1 x$ since $P(H) = 0$.

The computations for r_2, r_4, r_5 in case (Cb) are very complicated due to the co-product formula in $\Delta(y)$ and calculation in mod p . Here, we specify to case $(p = 2)$ and case $(p > 2)$ with additional assumption $gx = xg$.

Case (Cb) for $p = 2$: As before we have relations:

$$g^2 = 1, \quad gx - xg = \epsilon_1(g - g^2) = \epsilon_1(g - 1), \quad x^2 = \epsilon_1 x,$$

for $\epsilon_1 \in \{0, 1\}$; and working in mod 2

$$\begin{aligned} \Delta(gy - yg) &= (gy - yg) \otimes g + g \otimes (gy - yg) + \epsilon_1(x \otimes (g + 1) + (g + 1) \otimes xg) \\ &\quad + \epsilon_1(1 + g) \otimes (1 + g). \end{aligned}$$

One can check that $gy - yg - \epsilon_1(1 + g + x + xg)$ is (g, g) -primitive. This implies that $gy - yg = \epsilon_1(1 + g + x + xg)$. Also,

$$\Delta(xy - yx) = (xy - yx) \otimes 1 + g \otimes (xy - yx).$$

So $xy - yx = \sigma x + \tau(1 - g)$, for some $\sigma, \tau \in \mathbf{k}$, and

$$\Delta(y^2) = y^2 \otimes 1 + 1 \otimes y^2 + \tau((1 - g) \otimes x + xg \otimes (1 - g)) + \epsilon_1 xg \otimes x.$$

So $y^2 = \epsilon_1 y + \tau(x + xg)$. By Diamond Lemma [7], we get all compatible conditions as: $\sigma\tau = \sigma^2 - \epsilon_1\sigma = \epsilon_1\sigma = 0$. So we have $\sigma = 0$ and the relations are

$$\begin{aligned} g^2 &= 1, \quad gx - xg = \epsilon_1(g - 1), \quad gy - yg = \epsilon_1(1 + g + x + xg), \\ xy - yx &= \tau(1 - g), \quad x^2 = \epsilon_1 x, \quad y^2 = \epsilon_1 y + \tau(x + xg). \end{aligned}$$

If $\epsilon_1 = 0$, by rescaling x, y , we can choose $\tau \in \{0, 1\}$, where we get two classes of H . If $\epsilon_1 = 1$, we get one infinite family of H whose structures depending on $\tau \in \mathbf{k}$.

Case (Cb) for $p > 2$ with additional assumption: Suppose $[g, x] = 0$. We can get that $x^p = 0$ and

$$\Delta(gy - yg) = (gy - yg) \otimes g + g \otimes (gy - yg).$$

This implies that $gy = yg$. And

$$\Delta(xy - yx) = (xy - yx) \otimes 1 + g \otimes (xy - yx).$$

So $(xy - yx)$ is $(1, g)$ -primitive. By rescaling of x , which is also $(1, g)$ -primitive, we can write $xy - yx = \epsilon_2 x + \tau(1 - g)$, for some $\tau \in \mathbf{k}$ and $\epsilon_2 \in \{0, 1\}$.

Let A be the commutative Hopf subalgebra of H generated by $\{g, x\}$. We follow the notations in [16] to denote, depending on the context, $\rho_y = (\text{ad } y)$ as the right adjoint action of y on A , or $\rho_y = (\text{ad } (y \otimes 1 + 1 \otimes y))$ as the right adjoint action of $(y \otimes 1 + 1 \otimes y)$ on $A \otimes A$. Then by 2.3.1, one sees that

$$\Delta(y^p) = \left(y \otimes 1 + 1 \otimes y + \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{p-i} \otimes x^{p-i} \right)^p$$

$$= y^p \otimes 1 + 1 \otimes y^p + \rho_y^{p-1} \left(\sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{p-i} \otimes x^{p-i} \right).$$

We apply the fact that $\rho_y(x) = [x, y] = \epsilon_2 x + \tau(1 - g)$.

$$\begin{aligned} & \rho_y \left(\sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{p-i} \otimes x^{p-i} \right) \\ &= \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} \rho_y(x^i) g^{p-i} \otimes x^{p-i} + \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{p-i} \otimes \rho_y(x^{p-i}) \\ &= \epsilon_2 i \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{p-i} \otimes x^{p-i} + \tau i \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^{i-1} (1-g) g^{p-i} \otimes x^{p-i} \\ &+ \epsilon_2 (p-i) \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{p-i} \otimes x^{p-i} + \tau (p-i) \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{p-i} \otimes x^{p-i-1} (1-g) \\ &= \tau \left(\sum_{0 \leq j \leq p-2} \binom{p-1}{j} g^{p-1-j} x^j \otimes x^{p-1-j} - \sum_{0 \leq j \leq p-2} \binom{p-1}{j} g^{p-j} x^j \otimes x^{p-1-j} \right. \\ &\quad \left. + \sum_{1 \leq j \leq p-1} \binom{p-1}{j} g^{p-j} x^j \otimes x^{p-1-j} - \sum_{1 \leq j \leq p-1} \binom{p-1}{j} g^{p-j} x^j \otimes g x^{p-1-j} \right) \\ &= \tau ([\Delta(x^{p-1}) - x^{p-1} \otimes 1] - g^p \otimes x^{p-1} + g x^{p-1} \otimes 1 + [-\Delta(g x^{p-1}) + g^p \otimes g x^{p-1}]) \\ &= \tau (\Delta(x^{p-1}(1-g)) - (x^{p-1}(1-g)) \otimes 1 - 1 \otimes (x^{p-1}(1-g))) \\ &= \tau \partial^1(x^{p-1}(1-g)), \end{aligned}$$

where $\partial^1 : A \rightarrow A \otimes A$ such that $\partial^1(a) = \Delta(a) - a \otimes 1 - 1 \otimes a$, for any $a \in A$. Next, we need the following result.

Claim: ρ_y and ∂^1 commute with each other.

Proof of claim. For any $a \in A$, we get

$$\begin{aligned} \rho_y \partial^1(a) &= \rho_y(\Delta(a) - a \otimes 1 - 1 \otimes a) \\ &= [\Delta(a) - a \otimes 1 - 1 \otimes a, y \otimes 1 + 1 \otimes y] \\ &= [\Delta(a), y \otimes 1 + 1 \otimes y] - [a, y] \otimes 1 - 1 \otimes [a, y] \\ &= [\Delta(a), y \otimes 1 + 1 \otimes y] + \sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{p-i} \otimes x^{p-i} - [a, y] \otimes 1 - 1 \otimes [a, y] \\ &= [\Delta(a), \Delta(y)] - [a, y] \otimes 1 - 1 \otimes [a, y] \\ &= \Delta([a, y]) - [a, y] \otimes 1 - 1 \otimes [a, y] \\ &= \partial^1([a, y]) = \partial^1(\rho_y(a)). \end{aligned}$$

□

Therefore, one sees that

$$\begin{aligned} \rho_y^{p-1} \left(\sum_{1 \leq i \leq p-1} \frac{(p-1)!}{i!(p-i)!} x^i g^{p-i} \otimes x^{p-i} \right) &= \rho_y^{p-2} (\tau \partial^1(x^{p-1}(1-g))) \\ &= \tau \partial^1((1-g)\rho_y^{p-2}(x^{p-1})), \end{aligned}$$

so

$$\Delta(y^p - \tau \rho_y^{p-2}(x^{p-1})(1-g)) = (y^p - \tau \rho_y^{p-2}(x^{p-1})(1-g)) \otimes 1 + 1 \otimes (y^p - \tau \rho_y^{p-2}(x^{p-1})(1-g)).$$

Since $P(H) = 0$, we get $y^p = \tau(1-g)\rho_y^{p-2}(x^{p-1})$. Since the ambiguity $[x, y^p] = 0$ is resolvable, we conclude that $0 = [x, \tau \rho_y^{p-2}(x^{p-1})(1-g)] = x(\text{ad } y)^p = \epsilon_2^p x + \epsilon_2^{p-1} \tau(1-g)$. Hence, $\epsilon_2 = 0$ and $\rho_y(x) = \tau(1-g)$. Moreover, we get

$$y^p = \tau(1-g)\rho_y^{p-2}(x^{p-1}) = (p-1)!(1-g)\tau^{p-1}(1-g)^{p-2}x = -\tau^{p-1}(1-g)^{p-1}x.$$

Thus the relations are

$$g^p = 1, \quad gx - xg = 0, \quad gy - yg = 0, \quad xy - yx = \tau(1-g), \quad x^p = 0, \quad y^p = -\tau^{p-1}(1-g)^{p-1}x.$$

When we apply the Diamond Lemma [7], all the ambiguities of the relations are resolvable and there is no ambiguity condition in this case. By rescaling of x and y , we can take $\tau \in \{0, 1\}$. There are two classes of H .

4.4. Liftings for Case (D).

Case (D1). It is clear that H is the quotient of the free algebra $\mathbf{k}\langle g, x \rangle$, where $x \in H$ is lifting of $a \in \text{gr } H$, subject to the relations

$$g^{p^2} = 1, \quad gx - xg = r_1, \quad x^p = r_2,$$

for some $r_1 \in H_0$ and $r_2 \in H_{p-1}$. The coalgebra structure is determined by

$$\Delta(g) = g \otimes g, \quad \Delta(x) = x \otimes 1 + g^\epsilon \otimes x,$$

where $g^\epsilon = 1, g$, or g^p . We compute

$$\Delta(r_1) = r_1 \otimes g + g^{\epsilon+1} \otimes r_1.$$

Since $r_1 \in H_0$, we can write $r_1 = \epsilon_1(g - g^{\epsilon+1})$, for $\epsilon_1 \in \{0, 1\}$.

$$\Delta(r_2) = (x \otimes 1 + g^\epsilon \otimes x)^p.$$

We have the following three cases depending on the values of ϵ :

- **(D1a)** Suppose $\epsilon = 0$. Then $P(H) = \mathbf{k}x$, $r_1 = 0$, and $r_2 = \lambda x$, for some $\lambda \in \mathbf{k}$. Thus, after checking all ambiguities and by Diamond Lemma, the relations in H are:

$$gx = xg, \quad x^p = \lambda x.$$

No ambiguity conditions occur for case (D1a). By rescaling of x , we can take $\lambda = \epsilon_2 \in \{0, 1\}$. We obtain two classes of H whose structures depending on ϵ_2 .

- **(D1b)** Suppose $\epsilon = 1$. Then by applying 4.0.2, we have $\Delta(x^p - \epsilon_1 x) = (x^p - \epsilon_1 x) \otimes 1 + g^p \otimes (x^p - \epsilon_1 x)$. Hence, $x^p - \epsilon_1 x = \lambda(1 - g^p)$, for some $\lambda \in \mathbf{k}$, and $r_2 = x^p = \epsilon_1 x + \lambda(1 - g^p)$. The possible relations in H are:

$$gx - xg = \epsilon_1(g - g^2), \quad x^p = \epsilon_1 x + \lambda(1 - g^p),$$

for $\epsilon_1 \in \{0, 1\}$ and some $\lambda \in \mathbf{k}$. By Diamond Lemma [7], all the ambiguities of the relations are resolvable. There is no ambiguity condition in this case. If $\epsilon_1 = 0$, by rescaling x , we can choose $\lambda \in \{0, 1\}$. There are two classes. Otherwise, when $\epsilon_1 = 1$, we obtain one infinite family of H whose structures depending on $\lambda \in \mathbf{k}$.

- **(D1c)** Suppose $\epsilon = p$. Observe that since $[-, x]$ is a derivation on $\mathbf{k}\langle g \rangle$, $[g^p, x] = pg^{p-1}[g, x] = 0$ in characteristic p , so $g^p x = xg^p$. We have

$$\Delta(r_2) = (x \otimes 1 + g^p \otimes x)^p = x^p \otimes 1 + (g^p)^p \otimes x^p = x^p \otimes 1 + 1 \otimes x^p,$$

since $g^{p^2} = 1$. Thus, $r_2 \in P(H) = 0$ implying $x^p = 0$. The relations in H are:

$$gx - xg = \epsilon_1(g - g^{p+1}), \quad x^p = 0,$$

for $\epsilon_1 \in \{0, 1\}$. By Diamond Lemma [7], all the ambiguities of the relations are resolvable. There is no ambiguity condition in this case. We make a remark that for $[g, x^p]$ we need to apply the identity $(g)(\text{ad } x)^n = \epsilon_1^{n-1}(1 - g^p)^{n-1}[g, x]$, for all $n \geq 1$, which can be proved inductively. Thus we obtain two classes of H whose structures depending on $\epsilon_1 \in \{0, 1\}$.

Case (D2). It is clear that H is the quotient of the free algebra $\mathbf{k}\langle g_1, g_2, x \rangle$, where $x \in H$ is lifting of $a \in \text{gr } H$, subject to the relations

$$g_1^p = 1, \quad g_2^p = 1, \quad g_1 x - x g_1 = r_1, \quad g_2 x - x g_2 = r_2, \quad x^p = r_3,$$

for some $r_1, r_2 \in H_0$ and $r_3 \in H_{p-1}$. The coalgebra structure is determined by

$$\Delta(g_i) = g_i \otimes g_i, \quad \text{for } i = 1, 2; \quad \Delta(x) = x \otimes 1 + g_1^\epsilon \otimes x,$$

where $g_1^\epsilon = 1$ or g_1 . As before,

$$\Delta(r_1) = r_1 \otimes g_1 + g_1^{\epsilon+1} \otimes r_1; \quad \text{and}$$

$$\Delta(r_2) = r_2 \otimes g_2 + g_1^\epsilon g_2 \otimes r_2.$$

Since $r_1, r_2 \in H_0$, and since we can rescale x only once, we may write $r_1 = \epsilon_1(g_1 - g_1^{\epsilon+1})$ and $r_2 = \tau(g_2 - g_1^\epsilon g_2)$, for $\epsilon_1 \in \{0, 1\}$ and some $\tau \in \mathbf{k}$. We have the following two cases depending on the value of ϵ :

- **(D2a)** Suppose $\epsilon = 0$. Then $P(H) = \mathbf{k}x$, $r_1 = 0$, $r_2 = 0$, and $r_3 = \lambda x$, for some $\lambda \in \mathbf{k}$. By Diamond Lemma [7], all the ambiguities of the relations are resolvable. The relations in H are:

$$g_1 x = x g_1, \quad g_2 x = x g_2, \quad x^p = \lambda x,$$

for some $\lambda \in \mathbf{k}$. By rescaling of x , λ can be chosen as $\epsilon_2 \in \{0, 1\}$. No ambiguity conditions occur for case (D2a). We obtain two classes of H whose

structures depending on ϵ_2 .

- **(D2b)** Suppose $\epsilon = 1$. Then by applying 4.0.2, we have $(r_3 - \epsilon_1 x)$ is primitive. This implies $r_3 = \epsilon_1 x$ since $P(H) = 0$. The relations in H are:

$$g_1 x - x g_1 = \epsilon_1 g_1 (1 - g_1), \quad g_2 x - x g_2 = \tau g_2 (1 - g_1), \quad x^p = \epsilon_1 x,$$

for $\epsilon_1 \in \{0, 1\}$ and some $\tau \in \mathbf{k}$. By Diamond Lemma [7], all the ambiguities of the relations are resolvable. The ambiguity $[g_2, x^p] = (g_2)(\text{ad } x)^p = (g_2)(\text{ad } x)$ can be checked by using 4.0.1 (3), where we take $\delta = (\text{ad } x)$. Then one sees that $\delta(g_1) = \epsilon_1(g_1 - g_1^2)$ and $\delta(g_2) = \tau g_2(1 - g_1)$. If $\epsilon_1 = 0$, then one may rescale x and assume $\tau = \epsilon_2 \in \{0, 1\}$; and we get two classes of H depending on ϵ_2 . If $\epsilon_1 = 1$, we get one infinite family of H whose structures depending on $\tau \in \mathbf{k}$ and $\epsilon_1 = 1$.

Acknowledgements: The main work of this paper results from the second author's visit to Northeastern University in March 2016. The second author is thankful for their hospitality.

REFERENCES

- [1] N. Andruskiewitsch and M. Graña, Braided Hopf algebras over nonabelian finite groups, *Bol. Acad. Nac. Cienc. (Córdoba)*, 63 (1999), 45–78.
- [2] N. Andruskiewitsch and H.-J. Schneider, Lifting of quantum linear spaces and pointed Hopf algebras of order p^3 , *J. Algebra*, 209 (1998), 658–691.
- [3] ———, Pointed Hopf algebras, *New Directions in Hopf Algebras, MSRI Publications*, 43 (2002).
- [4] ———, On the classification of finite-dimensional pointed Hopf algebras, *Ann. Math.*, 171 (2010), 375–417.
- [5] I. Angiono and A. G. Iglesias, Pointed Hopf algebras with standard braiding are generated in degree one, *Contemp. Math.*, 537 (2011), 57–70.
- [6] ———, Liftings of Nichols algebras of diagonal type II. All liftings are cocycle deformations, preprint, arXiv:1605.03113.
- [7] G. Bergman, The diamond lemma for ring theory, *Adv. Math.*, 29 (1978), 178–218.
- [8] S. Caenepeel and S. Dăscălescu, Pointed Hopf algebras of dimension p^3 , *J. Algebra*, 209 (1998), 622–634.
- [9] C. Cibils, A. Lauve and S. Witherspoon, Hopf quivers and Nichols algebras in positive characteristic, *Proc. Amer. Math. Soc.*, 137 (2009), 4029–4041.
- [10] N. Jacobson, *Lie Algebras*, Dover Publications Inc., New York, 1979.
- [11] J. Wang and I. Heckenberger, Rank 2 Nichols algebras of diagonal type over fields of positive characteristic, *SIGMA Symmetry Integrability Geom. Methods Appl.* (2015), Paper 011, 24 pp.
- [12] Y. Kashina, G. Mason and S. Montgomery, Computing the Frobenius-Schur indicator for abelian extensions of Hopf algebras, *J. Algebra*, 251 (2002), 888–913.
- [13] S. Majid, Crossed products by braided groups and bosonization, *J. Algebra*, 163 (1994), 165–190.
- [14] S. Montgomery, *Hopf Algebras and Their Actions on Rings*, CBMS Regional Conference Series in Mathematics, 82, Amer. Math. Soc., Providence, RI, 1993.
- [15] V. C. Nguyen, L. Wang and X. Wang, Classification of connected Hopf algebras of dimension p^3 I, *J. Algebra*, 424 (2015), 473–505.
- [16] V. C. Nguyen, L. Wang and X. Wang, Primitive deformations of quantum p -groups, preprint, arXiv:1505.02454.

- [17] W. D. Nichols and M. B. Zoeller, A Hopf algebra freeness theorem, *Amer. J. of Math.*, 111 no. 2 (1989), 381–385.
- [18] D. E. Radford, The structure of Hopf algebras with a projection, *J. Algebra*, 92 (1985), 322–347.
- [19] ———, *Hopf algebras*, Series on Knots and Everything, 49, World Scientific Publishing Co. Pte. Ltd., Singapore, 2012.
- [20] S. Scherotzke, Classification of pointed rank one Hopf algebras, *J. Algebra*, 319 (2008), 2889–2912.
- [21] D. Ştefan, Hochschild cohomology on Hopf Galois extensions, *J. Pure Appl. Algebra*, 103 (1995), 221–233.
- [22] D. Ştefan and F. van Oystaeyen, Hochschild cohomology and the coradical filtration of pointed coalgebras: applications, *J. Algebra*, 210 (1998), 535–556.
- [23] D.-G. Wang, J. J. Zhang and G. Zhuang, Primitive cohomology of Hopf algebras, *J. Algebra*, 464 (2016), 36–96.
- [24] L. Wang and X. Wang, Classification of pointed Hopf algebras of dimension p^2 over any algebraically closed field, *Algebr. Represent. Theory*, 17 (2014), 1267–1276.
- [25] X. Wang, Connected Hopf algebras of dimension p^2 , *J. Algebra*, 391 (2013), 93–113.

DEPARTMENT OF MATHEMATICS, NORTHEASTERN UNIVERSITY, BOSTON, MA 02115

E-mail address: `v.nguyen@northeastern.edu`

DEPARTMENT OF MATHEMATICS, TEMPLE UNIVERSITY, PHILADELPHIA, PA, 19122-6094

E-mail address: `xingting@temple.edu`